1/2012

Datenschutz Nachrichten

35. Jahrgang
ISSN 0137-7767
9,00 Euro



■ EU-Datenschutz-Grundverordnung ■ Betriebliche und behördliche Datenschutzbeauftragte ■ Das Recht auf Vergessen ■ Warum wehren sich Menschen (nicht) gegen Verletzungen ihrer Datenschutzrechte? ■ Die Reform des europäischen Datenschutzrechts im Parlament ■ Facebook-Fanpages ■ Nachrichten ■ Rechtsprechung ■

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

Inhalt

Termine

Mittwoch, 18. April 2012
Datenschutz in der Medizin: Rechtliche und technische Entwicklungen im Gesundheitsbereich und ihre Relevanz für den Datenschutz
www.update-bdsg.com/html/18-04-2012.html

Montag – Freitag, 13.-17. Februar & 19.-23. März 2012
Weiterbildung für den Betriebsrat zur zertifizierten Fachkraft für Datenschutz bei SAP-Systemen
dtb – Datenschutz-und Technologieberatung Kassel
www.dtb-kassel.de

Freitag, 13 April 2012
DVD-Vorstandssitzung
Bielefeld. Anmeldung in der Geschäftsstelle
dvd@datenschutzverein.de

Freitag, 13. April 2012
Verleihung der BigBrotherAwards 2012
Bielefeld
http://www.bigbrotherawards.de

Dienstag – Donnerstag, 22. – 24. Mai 2012
Compliance oder Mitarbeiterkontrolle? Arbeitsrecht und Datenschutz
dtb – Datenschutz-und Technologieberatung Kassel
www.dtb-kassel.de

Freitag, 9. November 2012
FIfF Jahrestagung 2012
Hochschule Fulda
www.fiff.de

DANA
Datenschutz Nachrichten
ISSN 0137-7767
35. Jahrgang, Heft 1

Herausgeber
Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftstelle:
Rheingasse 8-10, 53113 Bonn
Tel. 0228-222498
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

Redaktion (ViSdP)
Karsten Neumann, Sönke Hilbrans
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Rheingasse 8-10, 53113 Bonn
dvd@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autoren.

Layout und Satz
Frans Jozef Valenta, 53119 Bonn
valenta@t-online.de

Druck
Wienands Printmedien GmbH
Linzer Str. 140, 53604 Bad Honnef
wienandsprintmedien@t-online.de
Tel. 02224 989878-0
Fax 02224 989878-8

Bezugspreis
Einzelheft 9 Euro. Jahresabonnement 32 Euro (incl. Porto) für vier Hefte im Jahr. Für DVD-Mitglieder ist der Bezug kostenlos. Das Jahresabonnement kann zum 31. Dezember eines Jahres mit einer Kündigungsfrist von sechs Wochen gekündigt werden. Die Kündigung ist schriftlich an die DVD-Geschäftsstelle in Bonn zu richten.

Leserbriefe
Leserbriefe sind erwünscht. Deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Abbildungen
Frans Jozef Valenta

Ein kleiner Schritt für Deutschland …

… ein großer Schritt für Europa – so lautet der durchaus ernst gemeinte Vergleich der Datenschutzgrundverordnung mit der berühmten ersten Mondlandung. Den Vergleich zog der Europäische Datenschutzbeauftragte Peter Hustinx am 26. Januar auf einer Veranstaltung der Europäischen Akademie für Informationsfreiheit und Datenschutz in Berlin. Die am Vortag veröffentlichten Vorschläge der EU-Kommission für die Neugestaltung des europäischen Datenschutz-Rechtsrahmens wollen den Datenschutz europaweit einheitlich, verbindlich, effektiv und zukunftssicher neu regeln. Für Deutschland ist das meiste bekannt, für andere europäische Länder ein Quantensprung. Das Paket ist mit einer Mitteilung, einer verbindlichen Verordnung und einer Rahmenrichtlinie für den Datenschutz in der polizeilichen und justiziellen Zusammenarbeit umfangreich und juristisch keine leichte Kost. Deshalb fällt es leicht, zwar berechtigter Weise einen fehlenden Rechtsschutz vor einem Europäischen Verfassungsgericht zu kritisieren, aber trotzdem völlig falsch zu liegen: dieser strukturelle Mangel gilt für die gesamte europäische Gesetzgebung seit dem Vertrag von Lissabon.

Entgegen den Prophezeiungen „gut unterrichteter Kreise“ hat sich die zuständige Kommissarin offensichtlich nicht nur terminlich, sondern auch inhaltlich als stark und entschlossen erwiesen. Vorausgegangen ist eine einjährige öffentliche Konsultation mit hunderten Stellungnahmen, auch der DVD. Die Lobbyarbeit geht nun in die nächste Runde. Das Parlament wird genauso wie beim ACTA-Vertrag zwischen wirtschaftlichen und bürgerrechtlichen Argumenten abwägen wollen. Die DVD wird gemeinsam mit anderen Datenschutz- und Bürgerrechtsorganisationen den Druck erhöhen, um im Europaparlament die deutlichen bürgerrechtlichen Fortschritte, die im Kommissionsentwurf liegen, so engagiert zu verteidigen, wie den Finger in die weiterhin offenen Wunden zu legen.

Aber bei aller berechtigten Kritik: die Mondlandung ist gelungen – auf dem Weg zurück zur Erde sollten alle auf riskante Flug- und Bremsmanöver verzichten.

Karsten Neumann

Autorinnen und Autoren dieser Ausgabe:

Dr. Alexander Dix
Beauftragte für Datenschutz und Informationsfreiheit des Landes Berlin
mailbox@datenschutz-berlin.de

Cornelia Ernst
Mitglied im Europäischen Parlament, cornelia.ernst@europarl.europa.eu

Werner Hülsmann
bis 2009 Vorstandsmitglied in der DVD, Mitglied des Beirats des Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e.V., selbständiger Datenschutzberater, externer Datenschutzbeauftragter und Datenschutzsachverständiger, Konstanz und Berlin, huelsmann@datenschutzverein.org.

Lorenz Krämer
Fachreferent im Büro von Cornelia Ernst (MdEP), lorenz.kraemer@europarl.europa.eu

Prof. Dr. Viktor Mayer-Schönberger
Lehrstuhlinhaber am Oxford Internet Institut, viktor.ms@oii.ox.ac.uk

Jeannette Spary
Assessorin jur., Wissenschaftliche Mitarbeiterin im Bundestagsbüro von Gerold Reichenbach, MdB, mit den Themenschwerpunkten Datenschutz und Netzpolitik, j.spary@web.de

Eric Töpfer
Wissenschaftlicher Mitarbeiter beim Deutschen Institut für Menschenrechte und Redakteur der Zeitschrift „Bürgerrechte und Polizei/CLIP“. toepfer@emato.de

Dr. Thilo Weichert
Leiter des Unabhängigen Landeszentrums für Datenschutz Schleswig Holstein, Kiel, weichert@datenschutzzentrum.de

Jeannette Spary

Die neue Datenschutz-Grundverordnung – Überblick und Problemaufriss

Am 25. Januar 2012 hat die EU-Justizkommissarin Viviane Reding die Entwürfe zu einer Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung, DS-GVO)[1] sowie zu einer Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr[2] in Brüssel vorgestellt. Die DS-GVO soll an die Stelle der Datenschutz-Richtlinie 95/46/EG treten, die von den 27 Mitgliedstaaten teils sehr unterschiedlich umgesetzt wurde.

Bereits im Dezember 2011 kursierten die ersten geleakten Entwürfe der DS-GVO und heizten die Diskussion an. Einen ersten Höhepunkt erreichte sie, als die Süddeutsche Zeitung einen Beitrag des Richters am Bundesverfassungsgericht Johannes Masing mit dem Titel „Ein Abschied von den Grundrechten" veröffentlichte.[3]

Hier sollen zunächst ein Überblick und erste Bewertung der DS-GVO erfolgen. Anschließend beschäftigt sich der Artikel mit der Frage, ob die Regelung und Harmonisierung des Datenschutzrechtes durch eine Verordnung oder besser weiterhin durch eine Richtlinie erfolgen sollte.

Was für Regelungen sind in der DS-GVO vorgesehen? Was ist neu?

Eine DS-GVO würde, anders als eine Richtlinie, unmittelbare Anwendung finden und das Recht der Mitgliedstaaten in ihrem Anwendungsbereich verdrängen. In Deutschland betrifft dies das Bundesdatenschutzgesetz (BDSG) und bereichsspezifisches Datenschutzrecht. Aber zunächst zu den Regelungen im Einzelnen.

- Der räumliche Anwendungsbereich (Art. 3) des europäischen Datenschutzrechts wird ausgeweitet. Die DS-GVO findet nicht nur auf Unternehmen Anwendung, die ihre Niederlassung in einem der Mitgliedstaaten haben. Sie richtet sich auch an solche Unternehmen, die ihren Sitz außerhalb der Europäischen Union haben, sich mit ihren Diensten aber an Nutzer und Verbraucher in der Europäischen Union wenden. Diskussionen über die Anwendbarkeit nationalen Rechts, wie sie derzeit mit beziehungsweise gegen facebook geführt werden, würden dadurch beendet.
- Die Rechte der Bürger werden gestärkt. Beispielsweise wird das Prinzip des Einwilligungserfordernisses gestärkt. Art. 7 enthält hier insoweit verheißungsvolle Ansätze, als nun ausdrücklich geregelt wird, dass die Einwilligung keine Rechtsgrundlage für die Verarbeitung personenbezogener Daten bieten kann, wenn zwischen der Position der betroffenen Person und des für die Verarbeitung Verantwortlichen ein erhebliches Ungleichgewicht besteht. Dies dürfte positive Auswirkungen auf die beim Beschäftigtendatenschutz geführte Debatte haben, ob eine freiwillige Zustimmung zu der Verarbeitung personenbezogener Daten hier nicht denklogisch ausgeschlossen ist. Vorgesehen ist weiter ein „right to be forgotten" (Art. 17). Während derzeit gilt „Das Internet vergisst nichts", soll der Nutzer in Zukunft die Möglichkeit haben, eine Zustimmung zurückziehen zu können und ein Recht auf Löschung haben. Nicht zuletzt soll es ein Recht auf Datenportabiliät (Art. 18) geben, das heißt, der Nutzer soll bei einem Anbieterwechsel seine Daten mitnehmen können. Dies sind innovative Vorschläge der Kommission, die zu einem Mehr an Verbraucherschutz führen würden.
- Die Prinzipien privacy by design/privacy by default (Art. 23) sollen gesetzlich verankert werden. Danach müssen alle Produkte und Dienstleistungen bei Auslieferung beziehungsweise bei der ersten Inanspruchnahme datenschutzfreundlich voreingestellt sein. Regelungsziel ist, dass nur so viele Daten erfasst, verarbeitet und gespeichert werden, wie für die Nutzung tatsächlich erforderlich ist.
- Die Verordnung soll nicht nur zu mehr Rechtssicherheit für die für Verarbeitung Verantwortliche, insbesondere Unternehmen, führen. Es sind auch mehr Sorgfaltspflichten (Art. 31, 79) vorgesehen. So sind sie bei einer Verletzung des Schutzes personenbezogener Daten dazu verpflichtet, die Aufsichtsbehörde unverzüglich zu benachrichtigen. Auch die betroffene Person muss benachrichtigt werden, wenn die Gefahr besteht, dass ihre Privatsphäre beeinträchtigt wird. Weiter werden die Sanktionsmöglichkeiten gegen Unternehmen verschärft. Die Aufsichtsbehörde kann eine Geldbuße bis zu 1.000.000 EUR respektive zwei Prozent des weltweiten Jahresumsatzes eines Unternehmens verhängen.[4]

Dem Bundesbeauftragten für Datenschutz, Peter Schaar, ist beizupflichten: es ist ein Entwurf mit Licht und Schatten. Neben deutlichen Verbesserungen gegenüber der derzeitigen Rechtslage gibt es Punkte, die noch nachgebessert werden müssen.

Welche Punkte sind problematisch?

- Ein betrieblicher Datenschutzbeauftragter soll erst ab einer fixen Betriebsgröße von 250 Mitarbeitern zu bestellen sein (Art. 35). Im BDSG ist die Bestellung eines Datenschutzbeauftragten schon dann vorgesehen, wenn in privaten

Unternehmen mindestens neun Personen ständig mit der Verarbeitung personenbezogener Daten betraut sind. Es liegt auf der Hand, dass das Risikopotential für die Verletzung des Schutzes personenbezogener Daten nicht von der Größe der verantwortlichen Stelle abhängt. Diese Regelung lädt jedoch zur Flucht ins Outsourcing und in die Gründung kleiner Subunternehmen ein.

- Verändert werden soll auch die Struktur von und die Zusammenarbeit der nationalen Datenschutzbehörden (Art. 46 ff.). Für Organisationen und Unternehmen soll eine einzige, von den Mitgliedstaaten festzulegende Aufsichtsbehörde Ansprechpartnerin sein. EU-Bürger sollen sich künftig auch an die Datenschutzbehörde ihres Landes wenden können, wenn ihre Daten von einem außerhalb der EU niedergelassenen Unternehmen verarbeitet werden. Die Aufsichtsbehörden sollen verwaltungsrechtliche Sanktionen verhängen können, wobei sich die Höhe der Geldbuße nach Art, Schwere und Dauer des Vorstoßes sowie der Frage nach Vorsatz oder Fahrlässigkeit bemisst. Die letztinstanzliche Aufsicht liegt bei der Europäischen Kommission. Das ist nicht unproblematisch. Denn auf der einen Seite soll die Unabhängigkeit der nationalen Datenschutzbehörden gestärkt werden, auf der anderen Seite bestehen weitgehende Befugnisse der Kommission zur Kontrolle. Die Kommission erhebt sich also selbst zur letzten unabhängigen Instanz in der Datenschutzaufsicht.
- In dem Entwurf finden sich zahlreiche Ermächtigungsgrundlagen für delegierte Rechtsakte der Kommission. Beispielsweise wird in Art. 23 Abs. 2 das Prinzip privacy by design/by default in der Verordnung verankert, im nächsten Absatz die genaue Ausgestaltung aber der Kommission vorbehalten, ohne dass ihre konkrete Rechtsform oder der genaue Inhalt vorher feststehen.
- Kinder und Jugendliche sollen besser geschützt werden. Aus diesem Grund ist gemäß Art. 8 für die Verarbeitung personenbezogener Daten eines Kindes bis zum vollendeten dreizehnten Lebensjahr die Einwilligung der Eltern erforderlich. Die Zielsetzung ist natürlich zu begrüßen. Fraglich ist nur, ob die Vollendung des dreizehnten Lebensjahres als Grenze nicht zu niedrig gesetzt ist und wie das Alter im Internet wirksam verifiziert werden soll. Im Zweifel werden weitere Daten erhoben werden müssen, um das Alter des Nutzers verlässlich feststellen zu können.
- Die in den letzten zwei Jahren intensiv geführte Debatte um den Beschäftigtendatenschutz erhält durch die Verordnung, abgesehen von der Frage der Einwilligung, leider keine neue Orientierung. In Art. 82 heißt es lediglich, dass die Regelungen zu diesem Punkt den Mitgliedstaaten überlassen bleiben, diese sich aber in den Grenzen dieser Verordnung bewegen müssen. Auch hier ist wieder viel Spielraum, wo sich die Mitgliedsstaaten, die Unternehmen und vor allem die Beschäftigten selbst mehr Klarheit und deutlichere Vorgaben gewünscht hätten.

Rechtschutz?

Eine europäische Harmonisierung des Datenschutzrechts ist wichtig und sinnvoll. Sowohl die einzelnen Regelungen als auch die Wahl der Rechtsform sind aber insbesondere bei einem so dynamischen Bereich wie dem Datenschutz mit all ihren Konsequenzen zu durchdenken. Die Entscheidung für eine Verordnung könnte Auswirkungen auf die Rechtsprechung des Bundesverfassungsgerichts (BVerfG) zu dem Verhältnis Gemeinschaftsrecht und nationales Recht haben. Das BVerfG geht seit der Solange-II-Entscheidung[5] von einem sogenannten Kooperationsverhältnis aus, d.h. es übt seine Prüfungskompetenz solange nicht aus, wie es generell auf europäischer Ebene einen gleichwertigen Grundrechtsschutz als gewährleistet ansieht. Dies wurde durch den Bananenmarkt-Beschluss[6] noch bekräftigt. Danach sind Verfassungsbeschwerden und Vorlagen von Gerichten, die eine Verletzung von Grundrechten durch sekundäres Gemeinschaftsrecht geltend machen, von vornherein unzulässig, wenn nicht begründet wird, dass der europäische Grundrechtsschutz unter den erforderlichen Standard gesunken ist. Es muss also detailliert dargelegt werden, dass der Grundrechtsschutz auf europäischer Ebene generell nicht mehr gewährleistet wird, was seit Verankerung der europäischen Grundrechtecharta nicht so schnell erfüllt sein dürfte.

Wird eine datenschutzrechtliche Entscheidung durch eine nationale Behörde getroffen, so gilt zunächst auch weiterhin das innerstaatliche Rechtsschutzsystem. Gelangen dann deutsche Fachgerichte bei der Überprüfung nationaler Umsetzungs- oder Durchführungsmaßnahmen zu der Überzeugung, dass der unabdingbare Standard des Grundgesetzes verletzt wurde oder die Union ihre Kompetenzen überschritten hat, kann und muss das Gericht gem. Art. 267 AEUV diese Frage dem EuGH vorlegen und diesem Gelegenheit geben, über die Gültigkeit des Unionsrechts zu entscheiden. Kommt das Fachgericht dem nicht nach, stellt dies einen Verstoß gegen das Recht auf den gesetzlichen Richter gemäß Art. 101 Abs. 1 S. 2 GG dar, was – unter zugegebenermaßen hohen Hürden – eine Verfassungsbeschwerde vor dem BVerfG begründen kann. Legt das Fachgericht vor, prüft der EuGH die vorgelegte Frage unter Berücksichtigung der Rechtsauffassung des vorlegenden Gerichts und gibt die Antwort zurück. Das vorlegende Gericht ist an die Auslegung des EuGH gebunden und muss unter diesem Gesichtspunkt entscheiden. Hat es Zweifel an der Entscheidung des EuGH, kann es den Fall unter Darlegung seiner Auffassung erneut vorlegen.

Verschlechtert sich also der Rechtsschutz durch eine Verordnung?

Entscheiden sich die Mitgliedstaaten für eine Verordnung, ist für deren Auslegung nicht primär das Bundesverfassungsgericht, sondern der Europäische Gerichtshof zuständig. Das BVerfG hat eine herausragende Rolle bei der Entwicklung des Datenschutzrechtes in Deutschland inne. Aber auch der EuGH hat sich bereits mehrfach mit dem Datenschutz auseinandergesetzt und diesem ebenfalls eine große Bedeutung beigemessen. Hier sei beispielsweise das Urteil zur Veröffentlichung von Empfängern von Agrarsubventionen genannt.[7] Zugegeben sei an dieser Stelle, dass der EuGH, anders als das BverfG, immer auch den Binnenmarkt im Auge haben wird. Entscheidungen wie die vorgenannte zeigen aber, dass ein Ausgleich zwischen den Interessen möglich und ge-

wollt ist, ohne dass der Datenschutz darunter leidet.

Knackpunkt bei der Diskussion scheint das Urteil des EuGH vom 24. November 2011[8] zu sein, in dem es um die Frage der Vereinbarkeit spanischen Rechts mit der Datenschutzrichtlinie von 1995 ging. Hier hat der EuGH entschieden, dass die Harmonisierung der nationalen Rechtsvorschriften durch die Richtlinie nicht auf eine Mindestharmonisierung beschränkt ist, über deren Schutzniveau die Mitgliedstaaten hinausgehen können, sondern vielmehr eine Vollharmonisierung darstellt. Aus diesem Grund würde sich das BVerfG sowohl bei einer umfassenden Richtlinie mit wenig Umsetzungsspielraum als auch bei einer Verordnung vor das Problem gestellt sehen, ob es an seiner Solange II-Rechtsprechung festhält.

Macht das Bundesverfassungsgericht derzeit von seiner Überprüfungskompetenz keinen Gebrauch, solange ein ausreichender Grundrechtsschutz auf europäischer Ebene gewährleistet wird, kann sich dies bei einem so grundrechts- und eingriffsrelevanten Bereich wie dem Datenschutz anders darstellen. Ist das Bundesverfassungsgericht der Ansicht, dass hier Grundrechtsstandards unterwandert würden, und die Anwendung der Unionsvorschriften in Deutschland verfassungswidrig wäre, müsste es zu dem Ergebnis kommen, dass europäisches Recht in diesem Fall in Deutschland nicht anwendbar ist.

Das BVerfG hat jedoch bereits anerkannt, dass generell einer ausreichender Grundrechtsschutz auf europäischer Ebene gewährleistet wird. Die europäische Grundrechtecharta wurde mit der Verankerung der Menschenwürde und des Grundrechts auf Datenschutz insbesondere aus Deutschland geprägt. Besonders grundrechtssensible Bereiche wie der Beschäftigtendatenschutz oder der Umgang mit Gesundheitsdaten sind zudem von der DS-GVO ausgenommen. Die Regelung dieser Bereiche wird explizit den Mitgliedsstaaten überlassen. In diesen grundrechtsintensiven Bereichen würde es also nicht zu einer Veränderung des innerstaatlichen Rechtschutzes kommen. Die nationalen Gerichte, und damit auch das BVerfG, blieben zuständig.

Fazit

Die Frage ist nicht mehr, ob wir die europäische Harmonisierung brauchen oder nicht, sondern auf welchem Niveau die Harmonisierung in Zukunft stattfindet. Ob die Harmonisierung durch eine Verordnung oder durch eine Richtlinie erfolgt, sollte weniger abstrakt beurteilt, sondern von den konkreten Inhalten abhängig gemacht werden. Eine Verordnung kann genauso noch Spielraum für die Mitgliedstaaten lassen, wie eine Richtlinie so detaillierte Vorgaben machen kann, dass de facto kein Umsetzungsspielraum mehr bleibt. Die Richtlinie von 1995 hält für neue technische Entwicklungen keine überzeugenden Antworten mehr bereit. Zudem führen die unterschiedlichen nationalen Regelungen zu Rechtsunsicherheit sowohl bei Unternehmen als auch bei Verbrauchern. Eine in allen Mitgliedstaaten unmittelbar wirkende DS-GVO könnte nicht nur zu mehr Rechtssicherheit, sondern auch zu einer Stärkung des Binnenmarkt-Prinzips führen, indem sich Unternehmen nicht mehr in dem Mitgliedsstaat niederlassen, wo das für sie vermeintlich günstigste Datenschutz-Recht gilt. Viele der genannten Regelungen stellen bereits ein Plus an Daten- und Verbraucherschutz dar. Dies gilt sowohl für die Frage der räumlichen Anwendbarkeit, des Prinzips privacy by default als auch des Rechts auf Datenportabilität. Nachgebessert werden kann und sollte immer, insbesondere bei den Punkten Bestellung eines betrieblichen Datenschutzbeauftragten, den delegierten Rechtsakten und der Struktur der Datenschutzaufsicht. Der Streit um die Rolle des BVerfG bei einer Richtlinie mit sehr geringem Umsetzungsspielraum für die Mitgliedstaaten nach dem EuGH-Urteil vom 24. November 2011[9] oder bei einer Verordnung ist dabei eher akademischer Natur.

1 KOM 2012 (11) endg.

2 KOM 2012 (10) endg.

3 Süddeutsche Zeitung v. 08.01.2012, Johannes Masing, Ein Abschied von den Grundrechten

4 Vor der Veröffentlichung des offiziellen Entwurf waren Sanktionsmöglichkeiten in Höhe von vier bis fünf Prozent des weltweiten Jahresumsatzes im Gespräch, so dass hier die Lobbyarbeit amerikanischer und europäischer Wirtschaftsunternehmen bereits erste Früchte getragen haben dürfte.

5 BVerfG, 22.10.1986 - 2 BvR 197/83

6 BverfG, 07.06.2000 – 2 BvL 1/97

7 EuGH,Urteil vom 09.11.2010 - C-92/09; C-93/09

8 EuGH, Urteil vom 24.11.2011, C-468/10 und C 469/10

9 EuGH, Urteil vom 24.11.2011, C-468/10 und C 469/10

Cartoon



Werner Hülsmann

Der betriebliche und behördliche Datenschutzbeauftragte im Entwurf der EU-Datenschutz-Grundverordnung

Im Entwurf der Datenschutz-Grundverordnung (DS-GVO-E) ist der Abschnitt 4 mit den Artikel 35 bis 37 dem betrieblichen bzw. behördlichem Datenschutzbeauftragten (DSB) gewidmet. Die Institution des betrieblichen oder behördlichen Datenschutzbeauftragten wird mit dem Inkrafttreten der DS-GVO in den meisten Staaten erstmalig eingeführt. In Deutschland gibt es dagegen eine jahrzehntelange Praxis hierzu.

Artikel 35 – Benennung eines Datenschutzbeauftragten

Absatz 1

Für Behörden und öffentliche Einrichtungen ist die Regelung, wann ein Datenschutzbeauftragter zu bestellen („benennen") ist, in Art. 35 Abs. 1 Buchstabe a) einfach und eindeutig: Sobald personenbezogene Daten verarbeitet werden, ist ein Datenschutzbeauftragter zu bestellen.

Für nichtöffentliche Einrichtungen ist in Art. 35 Abs. 1 Buchstaben b) und c) vorgegeben, wann ein Datenschutzbeauftragter zu bestellen ist. Gemäß Art. 35 Abs. 1 Buchstabe b) ist von Unternehmen ein Datenschutzbeauftragter zu bestellen, wenn die verantwortliche Stelle („der für die Datenverarbeitung Verantwortliche") oder der Datenverarbeiter im Auftrag („Auftragsverarbeiter") 250 oder mehr Mitarbeiter beschäftigt.

Der dritte Grund ist dagegen nicht so klar und zudem in den Erläuterungen anders formuliert als im Text des Artikels 35:

Während es bei der Formulierung der Erläuterungen um Verarbeitungsvorgänge geht, die einer regelmäßigen, systematischen Überwachung bedürfen, geht es bei dem Text von Art. 35, Abs. 1 Buchstabe c) um die Betroffenen, deren regelmäßige und systematische Beobachtung erforderlich für die Verarbeitungsvorgänge sein muss. Dabei müssen diese Verarbeitungsvorgänge auch noch zur Kerntätigkeit der verantwortlichen Stelle bzw. des Auftragsverarbeiters gehören. Die Formulierung der Erläuterung wäre in etwa vergleichbar mit den Anforderungen, wann eine Vorabkontrolle nach § 4d Abs. 5 BDSG vorgenommen werden muss. Zur Interpretation der Formulierung im Artikel kann der Erwägungsgrund 75 herangenommen werden:

„In Fällen, in denen die Verarbeitung im öffentlichen Sektor oder durch ein privates Großunternehmen erfolgt oder in denen die Kerntätigkeit eines Unternehmens ungeachtet seiner Größe Verarbeitungsvorgänge einschließt, die einer regelmäßigen und systematischen Überwachung bedürfen, sollte der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter bei der Überwachung der unternehmensinternen Einhaltung der Bestimmungen dieser Verordnung von einer weiteren Person unterstützt werden. Derartige Datenschutzbeauftragte sollten unabhängig davon, ob es sich um Angestellte des für die Verarbeitung Verantwortlichen handelt oder nicht, ihre Pflichten und Aufgaben in vollständiger Unabhängigkeit ausüben können."

Auch dieser Erwägungsgrund lässt die Vermutung zu, dass der Text von Art. 35 Abs. 1 Buchstabe c) fehlerhaft ist.

Unter der Annahme, dass die Formulierung aus dem Erwägungsgrund 75 und der Erläuterung zu Artikel 35 das darstellt, was im Entwurf der DS-GVO zur Benennung der Datenschutzbeauftragten geregelt werden soll, und dass die Verarbeitungen, die *„die einer regelmäßigen und systematischen Überwachung bedürfen"* in etwa denen entsprechen, die nach § 4d Abs. 5 BDSG einer Vorabkontrolle bedürfen, ist davon auszugehen, dass viele der Unternehmen, die derzeit nach § 4f BDSG einen Datenschutzbeauftragten bestellt haben, auch künftig einen Datenschutzbeauftragten benennen müssen. Allerdings wird die Anzahl der Unternehmen in Deutschland, die nach Art. 35 Abs. 1 einen Datenschutzbeauftragten benennen müssen, deutlich geringer sein, als die Anzahl der Unternehmen die nach § 4f BDSG einen Datenschutzbeauftragten bestellen müssen.

Leider zeigt die Erfahrung, dass entgegen der klaren Formulierung in § 4g Abs. 2a BDSG viele Geschäftsführer und

Artikel 35	Erläuterungen zu Artikel 35
1. Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter benennen einen Datenschutzbeauftragten, falls (…) oder c) die Kerntätigkeit des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihres Wesens, ihres Umfangs und/oder ihrer Zwecke eine regelmäßige und systematische Beobachtung von betroffenen Personen erforderlich machen.	Artikel 35 schreibt die Einsetzung eines Datenschutzbeauftragten für (…) und in Fällen vor, in denen die Kerntätigkeit des für die Verarbeitung Verantwortlichen oder des Auftragverarbeiters aus Verarbeitungsvorgängen besteht, die einer regelmäßigen, systematischen Überwachung bedürfen.

Inhaber meinen, dass sie sich nicht um den Datenschutz kümmern müssten, wenn sie keinen Datenschutzbeauftragten bestellen müssen. Wenn hier die Kapazitäten der bundesdeutschen Aufsichtsbehörden nicht deutlich erhöht werden – und deutlich häufiger Datenschutzkontrollen durchgeführt werden, wird diese eindeutig zu hoch angesetzte Zahl von 250 Mitarbeitern, ab der ein Datenschutzbeauftragter zu bestellen ist, dazu führen, dass in vielen Unternehmen der Datenschutz noch mehr an Bedeutung verlieren wird.

Absatz 2

Abs. 2 regelt ausdrücklich, dass es Konzerndatenschutzbeauftragte geben kann, indem eine Gruppe von Großunternehmen, also eine Gruppe von Unternehmen mit jeweils mehr 250 Mitarbeitern, einen gemeinsamen Datenschutzbeauftragten bestellen darf. Für eine Bestellung die nach Buchstabe c) zu erfolgen hat, gilt Absatz 2 nicht. In der Praxis gab und gibt es auch bisher in Deutschland Konzerndatenschutzbeauftragte, auch wenn sie formal von (fast) jedem Unternehmen des Konzerns eigenständig bestellt worden sind.

Absatz 3

Absatz 3 regelt, dass mehrere Behörden und öffentliche Einrichtungen entsprechend ihrer Struktur einen Datenschutzbeauftragten für mehrere Bereiche bestellen können. Dies stellt keine Änderung gegenüber den bereits jetzt in Deutschland geltenden Regelungen auf Bundes- und Länderebene dar.

Absatz 4

Absatz 4 erlaubt die Bestellung eines Datenschutzbeauftragten ausdrücklich auch dann, wenn die Bedingungen aus Absatz 1 nicht erfüllt sind.

Absatz 5

Absatz 5 formuliert Mindestanforderungen an die berufliche Qualifikation und das Fachwissen, die sich – ähnlich wie im BDSG – vor allem nach der Art der Datenverarbeitung und dem Schutzbedarf richten.

Absatz 6

In Absatz 6 wird erfreulicher Weise deutlich gemacht, dass es keine Interessenkonflikte zwischen der Aufgabenerfüllung als Datenschutzbeauftragter und sonstigen Tätigkeiten im Unternehmen oder der Behörde geben darf. Dies gilt bereits auch nach deutschem Datenschutzrecht. Allerdings nur über den Umweg, dass das Vorhandensein von Interessenkonflikten von den Aufsichtsbehörden als mangelnde Zuverlässigkeit ausgelegt wird.

Absatz 7

Absatz 7 legt fest, dass ein Datenschutzbeauftragter für mindestens zwei Jahre zu benennen ist und in seiner Amtszeit nur von seinem Amt enthoben werden kann, „wenn er die Voraussetzungen für die Erfüllung seiner Pflichten nicht mehr erfüllt“. Eine Benennung für weitere Amtszeiten wird ausdrücklich für zulässige erklärt.

Das BDSG nennt keine Mindestfristen für die Bestellung als Datenschutzbeauftragter. Bei externen Datenschutzbeauftragten erwarten die Aufsichtsbehörden allerdings eine Mindestbestellung von drei bis fünf Jahren. Bei internen Datenschutzbeauftragten, bei denen der zum 01. September 2009 eingeführte Kündigungsschutz greift, gehen einige Unternehmen inzwischen auch dazu über, den Datenschutzbeauftragten nur befristet zu bestellen. Auch wenn es hierzu keine Regelung im BDSG gibt, wird dies von den Aufsichtsbehörden toleriert, solange die Dauer der Befristung ausreichend lange ist, um die unabhängige Aufgabenerfüllung zu gewährleisten. Bei einem Mindestzeitraum von zwei Jahren, wie ihn der aktuelle Verordnungsentwurf vorsieht, ist die unabhängige Aufgabenerfüllung nicht sicher gestellt. Die Praxis zeigt, dass auch bei Vorliegen der erforderlichen beruflichen Qualifikation und des nötigen Fachwissens, die Tätigkeit als neuer Datenschutzbeauftragter in einem Unternehmen eine gewisse Einarbeitungszeit bedarf. Sollte ein Unternehmen alle zwei Jahre einen neuen Datenschutzbeauftragten bestellen, so wäre eine kontinuierliche Aufgabenerfüllung schlicht nicht möglich.

Absatz 8

Absatz 8 regelt explizit, dass Datenschutzbeauftragte nicht bei der verantwortlichen Stelle oder dem Auftragsverarbeiter beschäftigt sein müssen, sondern die Tätigkeit auch auf Basis eines Dienstvertrages erbringen können. Allerdings sind hier keine Regelungen zu Berufsgeheimnisträgern, wie Ärzten und Rechtsanwälten enthalten. Im BDSG wurden 2006 solche Regelungen explizit eingeführt um klarzustellen, dass der aufgabenbedingte Zugriff auf Patienten- oder Mandantendaten keine Verletzung des Privatgeheimnisses nach § 203 StGB darstellt. Ohne entsprechende Anpassungen entweder in der Verordnung oder im nationalen Recht (z.B. durch Klarstellung im § 203 StGB) wäre diese Formulierung ein Rückschritt vor 2006.

Absatz 9

Durch Absatz 9 wird – die leider im BDSG nicht vorhandene – Pflicht eingeführt, Namen und Kontaktdaten des Datenschutzbeauftragten der Aufsichtsbehörde und der Öffentlichkeit mitzuteilen. Ohne die Kenntnis zumindest der Kontaktdaten ist die direkte Ansprache des Datenschutzbeauftragten durch einen Betroffenen kaum möglich. Daher ist diese Regelung sehr zu begrüßen.

Absatz 10

Gemäß Absatz 10 können sich Betroffene, wie es bereits auch im § 4f Abs. 5 Satz 2 BDSG geregelt ist, direkt an den Datenschutzbeauftragten wenden.

Absatz 11

Mit Absatz 11 wird der Kommission das Recht gegeben, durch „delegierte Rechtsakte“ zu erlassen „um die Kriterien und Anforderungen für die in Absatz 1 Buchstabe c genannte Kerntätigkeit des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters sowie die Kriterien für die berufliche Qualifikation des in Absatz 5 genannten Datenschutzbeauftragten festzulegen“.

Durch diese Regelung werden wesentliche Teile der Datenschutz-Grundverordnung nicht von der Verordnung selbst geregelt und damit durch den Ministerrat und das EU-Parlament beschlossen, sondern der Kommission überlassen. Nur wenn der Ministerrat oder das EU-Parlament innerhalb von zwei Monaten nach Mitteilung eines solchen Rechtsaktes durch die Kommission Einwände erhebt, tritt ein solcher

Rechtsakt nicht in Kraft. Daher sollten zumindest Mindestkriterien direkt in der Verordnung bestimmt werden.

Artikel 36 – Stellung des Datenschutzbeauftragten

Die in Artikel 36 enthaltenen Regelungen zur Stellung des Datenschutzbeauftragten (Unabhängigkeit, Weisungsfreiheit, direkter Bericht an die Leitung der Stelle, etc.) entsprechen den im BDSG enthaltenen Regelungen.

Artikel 37 – Aufgaben des Datenschutzbeauftragten

Während die Formulierungen in § 4g BDSG zu den Aufgaben des Datenschutzbeauftragten nur in einem Punkt, nämlich dem Vertrautmachen der Mitarbeiter mit den arbeitsplatzbezogenen Anforderungen des Datenschutzes, ausreichend konkret sind, stellt Artikel 37 des Entwurfs die Aufgaben deutliche konkreter dar. Insbesondere wird die Pflicht des Datenschutzbeauftragten, die verantwortliche Stelle bzw. den Auftragsverarbeiter über die Datenschutzverpflichtungen zu unterrichten und zu beraten, sowie diese Tätigkeit und die Antworten zu dokumentieren, ausdrücklich in seinen Aufgaben aufgeführt.

Sanktionen

Gemäß Art. 79 Abs. 6 Buchstabe j verhängt die Datenschutzaufsichtsbehörde ein Bußgeld in Höhe bis zu einer Millionen Euro oder bei Unternehmen bis zu 2% des weltweiten Jahresumsatzes gegen jeden, der vorsätzlich oder fahrlässig „*keinen Datenschutzbeauftragten nach Artikel 35 benennt oder nicht die Voraussetzungen für die Erfüllung seiner Aufgaben gemäß Artikel 35, 36 und 37 schafft*“.

Im Gegensatz zur aktuell geltenden Regelung in Deutschland gehört damit die Nichtbestellung eines erforderlichen Datenschutzbeauftragten zur Gruppe der schweren Verstöße mit den höchsten Bußgeldandrohungen. Dies ist aus Datenschutzsicht zu begrüßen.

Fazit

Die Regelungen zur Bestellung von Datenschutzbeauftragten stellen zwar für weite Teile der EU eine deutliche Erhöhung des allgemeinen Datenschutzniveaus dar, bedürfen aber ungeachtet dessen einer Überarbeitung. Hierbei sollten die Erfahrungen aus der Praxis sowohl interner und externer Datenschutzbeauftragter ebenso einfließen, wie die Erkenntnisse der Datenschutzaufsichtsbehörden. So müssen nicht nur unklare (und wie in Art. 35 Abs. 1 Buchstabe c) unrichtige) Formulierungen klarer gefasst werden, sondern auch die materiellen Regelungen insbesondere bezüglich der Mitarbeiterzahlen und der Mindestbestellfrist auf praxisbezogene Werte angepasst werden. Alle Mitarbeiter eines Unternehmens zu zählen, unabhängig davon, ob sie personenbezogene Daten verarbeiten oder nicht, ist genauso wenig hilfreich, wie die Anzahl der Mitarbeiter, ab der ein Datenschutzbeauftragter zu bestellen ist, willkürlich hoch zu setzen. Alle zwei Jahre einen neuen Datenschutzbeauftragten zu bestellen führt sicher nicht zur kontinuierlichen und unabhängigen Aufgabenerfüllung. Als Grundlage für konstruktive Diskussionen ist der Entwurf geeignet, zu un- oder nur geringfügig veränderten Verabschiedung dagegen nicht.

Viktor Mayer-Schönberger

Was uns Mensch sein lässt – Anmerkungen zum Recht auf Vergessen

Die Europäische Kommission machte Ende 2011 ihren Entwurf einer Verordnung des Parlaments und des Rates zum allgemeinen Datenschutz den am Rechtswerdungsprozess Beteiligten zugänglich. Rasch gelangte dieser Entwurf an die Öffentlichkeit und wurde seitdem von einer großen Zahl an Medien und Experten gleichermaßen analysiert und bewertet. Das Interesse ist verständlich; geht es doch um nichts weniger als eine Modernisierung des in die Jahre gekommenen allgemeinen Datenschutzes auf europäischer Ebene.

Einer der fünf von der Kommission bereits davor angekündigten Säulen dieser Modernisierung soll ein „Recht auf Vergessen“ sein. Erwartungskonform findet sich daher im Entwurf in Artikel 17 ein Recht auf Vergessen und Löschung. Um zu verstehen, warum der Kommission ein auf den ersten Blick sehr enger Aspekt des Datenschutzes – das Vergessen – einen Artikel wert ist, bedarf es zweierlei: 1. einen Blick auf die Rolle, die dem Vergessen und dem Erinnern in unserer Gesellschaft zukommt; und 2. ein Verständnis für die durch digitale Technologien geförderte Veränderungen im praktischen Vergessen und Erinnern.

In einem weiteren, dritten Schritt gehe ich dann auf die von der Kommission vorgeschlagene Implementation des Rechts auf Vergessen ein. Dabei ist zu Beginn eine Begriffsklärung notwendig: Vergessen und Erinnern bezeichnen in der Regel menschliche Vorgänge, die aber seit Jahrtausenden durch technische Hilfsmittel (z. B. Schrift) unterstützt werden. In unserer digitalen Welt umfasst das praktische Erinnern von Vergangenem geradezu regelmäßig ein Zusammenwirken von menschlichem

Geist und technischen Hilfsmitteln. In diesem Sinn versteht auch die Kommission die Begriffe, und ihr vorzuwerfen, sie hätte Vergessen und Erinnern semantisch falsch eingesetzt, negiert die Wirklichkeit.

1. Die Rolle von Erinnern und Vergessen:

In der Diskussion wird die Gefahr des fehlenden Vergessens oft auf eine Debatte um informationelle Ungleichgewichte verengt. Natürlich: Wenn andere Informationen über uns sammeln, speichern und wiederfinden können, lange nachdem wir selbst diese Informationen schon vergessen haben oder auch ohne dass wir von deren Existenz gewusst haben, dann verschiebt sich die informationelle Macht zugunsten dieser Informationssammler und zu Lasten der Betroffenen. Das aufzuzeigen ist notwendig, und auch ein tragfähiger Grund für ein Recht auf Vergessen einzutreten.

Aber das Vergessen erfüllt noch weitere Funktionen. Wir Menschen vergessen physiologisch die allermeisten Sinneseindrücke und Gedanken. Nur ein ganz kleiner Bruchteil dessen, was wir täglich erleben und denken bleibt in unserem Langzeitgedächtnis erhalten. Unser Gehirn arbeitet dabei informationsökonomisch effizient: gerade weil wir abstrahieren und zu allgemeinen Schlussfolgerungen befähigt sind, vergessen wir Details. Durch das Vergessen entledigen wir uns also zumeist jener Informationen, die unser Gehirn für unser Handeln und Sein in der Gegenwart als nicht relevant einstuft. Das mag manchmal daneben greifen (wenn wir nicht mehr erinnern, wo in einer großen Parkgarage wir unser Auto abgestellt haben), aber funktioniert im Wesentlichen erstaunlich gut. Im Gegenzug bedeutet dies: Wer sich an alles in seiner Vergangenheit erinnert, hat Schwierigkeiten im Hier und Heute zu leben und zu entscheiden; dafür ist die Vergangenheit zu präsent. Das bestätigen die einschlägigen Arbeiten führender Kognitionsforscher.

Wer in der Vergangenheit verhaftet bleibt, dem fällt es nicht nur schwer in der Gegenwart zu entscheiden, sondern auch sich selbst und sein Gegenüber als Menschen wahrzunehmen, die sich über die Zeit hinweg verändern. Erinnert man Menschen, dass ihr Gegenüber sie vor zehn Jahren belogen hat, misstrauen sie plötzlich ihrem Gegenüber auch in der Gegenwart. Umfassendes, stetes Erinnern lässt uns daher vergessen, dass wir alle uns verändern, unsere Meinungen wechseln, unsere Vorlieben, und mitunter auch unsere Werte. Wir verlernen so auch zu vergeben.

Stetes Erinnern erschwert es in der Gegenwart zu entscheiden, und uns selbst und unser Gegenüber als ein sich veränderndes Individuum wahrzunehmen. Es nimmt uns, wie der Schriftsteller Jorge Luis Borges formulierte, genau das, was uns Mensch sein lässt.

2. Das Vergessen in der digitalen Zeit:

Weil wir das Meiste vergessen, haben Menschen seit Jahrtausenden versucht Erinnerungen festzuhalten. Sprache, Schrift, und Malerei sind eindrückliche Beispiele, zu denen sich weitere Techniken wie Fotografie, Film und Tonaufzeichnung gesellten. Aber bis zum Beginn des digitalen Zeitalters blieb das Festhalten von Erinnerungen zeitaufwändig und teuer, und wurde daher mit Bedacht eingesetzt: vermeintlich wichtige Dinge wurden festgehalten, und das Vergessen blieb die Regel.

Im digitalen Zeitalter hat sich dies in zweifacher Hinsicht verändert. Zum Ersten sind digitale Speicher heute so kostengünstig, dass wir ohne Aufwand vieles oder alles in diesen Speichern festhalten können: jede Version eines Dokumentes, jedes Email, jedes noch so schlechte digitale Foto. Speichern ist heute kostengünstiger als Löschen: selbst fünf Sekunden unserer Zeit zu entscheiden, ob wir ein digitales Foto behalten oder löschen wollen, ist „teurer“, als dieses Foto zu speichern (und zu sichern). Da macht es auch ökonomisch wenig Sinn mehr, diese Speicher nicht zu nutzen.

Zum Zweiten ist heute das Wiederauffinden gespeicherter Informationen vergleichsweise einfach und intuitiv geworden. Wir müssen uns nicht mehr verkürzte Dateinamen aus acht Stellen merken, ja nicht einmal mehr Dateinamen an sich, weil wir ganz einfach unsere digitalen Speicher im Volltext durchsuchen können. Wir haben ein Jahrzehnt und mehr unsere Emails zur Verfügung und die Suchfunktion findet die zehn Jahre alten nur Bruchteile von Sekunden nach denen von letzter Woche. Am Internet ist es dank Google und Bing empfunden nicht anders. Das konfrontiert uns ständig mit vergessen Geglaubtem, an das wir dann durch die digitale Krücke wieder erinnern. Im digitalen Leben lässt uns die Vergangenheit nicht mehr los. Facebook hat daraus noch eine Dienstleistung gemacht.

Das aber kann genau zu den Konsequenzen eines steten Erinnerns führen, die ich oben skizziert habe. Genau deshalb lohnt es sich, darüber nachzudenken, wie man dem Vergessen auch in digitalen Zeiten wieder eine Chance geben kann – nicht um des Vergessens willen, sondern um unser selbst willen.

3. Das vorgeschlagene Recht auf Vergessen:

Der Kommissionsentwurf zu Artikel 17 (Recht auf Vergessen) enthält für Datenschutz-Experten jedenfalls auf den ersten Blick viel Vertrautes. Hier wird wiederholt und zusammengefasst, allenfalls ein wenig akzentuiert und konturiert, was schon in der Datenschutz-RL galt: klare Zweckbindung als Kriterium für die Speicherdauer, Verweis auf die Zustimmung der Betroffenen, Recht auf Löschung. Allenfalls mag die Kompetenzzuweisung an die Kommission zu sektoralen Sonderbestimmungen das Interesse wecken.

Das ist kein automatischer Makel. Es mag für die Rechtsunterworfenen, die sich bisher in der Komplexität der Datenschutz-RL nicht zurecht gefunden haben, vielleicht sinnvoller sein, thematisch bezogen alles an einer Stelle zu finden.

Interessant ist auch, wie Absatz 7 die Verarbeiter bewusst einbindet und auffordert, technische Vorkehrung für ein „Vergessen“ bei Zeitauflauf – intuitiv denkt man an ein Ablaufdatum - zu treffen. Verbunden mit den von der Kommission vorgesehenen erweiterten Möglichkeiten der Aufsichtsbehörde, kann sich hier eine durchaus interessante Dynamik entwickeln, die den Datenschutz langsam aber sicher

von seiner primären Bezogenheit auf Individualrechte der Zustimmung ablöst.

Genau das sehe ich als den sublim versteckten, aber vielleicht strukturell größten Innovations-Schritt des Kommissionsentwurfes. Hatten wir über Jahrzehnte versucht (und mit guten theoretischen Gründen!), die Verarbeitung personenbezogener Daten an die informierte Zustimmung der Betroffenen zu koppeln, so scheint sich nunmehr auch in der Kommission die Erkenntnis etabliert zu haben, dass dies alleine nicht ausreicht. Es geht nicht mehr vor allem um den Schutz *ex ante*, sondern – gerade weil so viel von uns auch selbst „verschuldet" online ist – gerade auch um den Schutz *ex post*. Das „Recht auf Vergessen" kann hier helfen, weil es ganz nahe an der Rechtswirklichkeit der Betroffenen die Notwendigkeit einer Korrektur *ex post* vor Augen hat: es soll bildlich gesprochen helfen, nachdem die Milch vergossen ist. Das ist nur zu begrüßen. Die Praxis wird zeigen, wie gut das klappt.

4. Fazit

Im Lichte der technischen Entwicklung und gesellschaftlichen Nutzung des Internets wird die Notwendigkeit verständlich, sich dem Vergessen in digitalen Zeiten auch aus legislativer Perspektive zu nähern. Das in Artikel 17 des Verordnungs-Entwurfes konkretisierte Recht auf Vergessen ist dazu ein erster evolutionärer, aber willkommener Schritt.

Eine weit detailliertere und deshalb auch differenziertere Argumentation findet sich in Viktor Mayer-Schönberger, Delete: Die Tugend des Vergessens in Digitalen Zeiten (Berlin University Press 2010).

Eric Töpfer

Warum wehren sich Menschen (nicht) gegen Verletzungen ihrer Datenschutzrechte?

Eine Studie der EU-Agentur für Grundrechte sucht Antworten

In Vorausschau auf das Inkrafttreten des Vertrages von Lissabon und die absehbare Novellierung des europäischen Datenschutzrechts schrieb der Rat der Europäischen Union der neu gegründeten EU-Agentur für Grundrechte im Jahr 2007 das Thema „Informationsgesellschaft und insbesondere Achtung der Privatsphäre und Schutz von personenbezogenen Daten" in ihren ersten Mehrjahresplan.[1]

Ziel der Grundrechteagentur, so ihr Gründungsdokument, ist es, der Gemeinschaft und ihren Mitgliedstaaten „bei der Durchführung des Gemeinschaftsrechts in Bezug auf die Grundrechte Unterstützung zu gewähren und ihnen Fachkenntnisse bereitzustellen, um ihnen die uneingeschränkte Achtung der Grundrechte zu erleichtern". Hierzu soll sie „relevante objektive, verlässliche und vergleichbare Informationen und Daten" sammeln, erfassen, analysieren und verbreiten, dafür Standards entwickeln, „wissenschaftliche Forschungsarbeiten und Erhebungen" durchführen" und „Schlussfolgerungen und Gutachten zu bestimmten Themen" ausarbeiten und veröffentlichen. Dies allerdings mit drei wesentlichen Einschränkungen: Den thematischen Rahmen der Tätigkeit der Agentur steckt der Rat mit Mehrjahresprogrammen ab, die auf Vorschlag der Kommission und nach Anhörung des Parlaments beschlossen werden. Zu Gesetzgebungsverfahren der EU darf die Agentur nur dann Stellung nehmen, wenn sie ausdrücklich von beteiligten Organen dazu aufgefordert wird. Auch befasst sie sich nicht mit der Frage der Rechtmäßigkeit von Handlungen der Unionsorgane oder Vertragsverletzungen durch Mitgliedstaaten.[2]

Nachdem die Grundrechteagentur 2008/2009 mit einer Stellungnahme zur Speicherung von Fluggastdaten und der Beteiligung an einer Konsultation der Kommission zu Körperscannern erste Schritte im Themenfeld Datenschutz gegangen war, legte sie 2010 eine größere vergleichende Studie zur Rolle der nationalen Datenschutzbehörden vor.[3] Als zentrale Probleme wurde damals die mangelnde Unabhängigkeit der Aufsichtsbehörden in einigen Ländern, ihre oftmals unzureichende Ausstattung und mitunter mangelnde Kompetenzen genannt. Des Weiteren wurden die defizitäre Durchsetzung bestehender Gesetze und der verbreitete Fokus auf „weiche" Instrumente kritisiert. Nicht zuletzt wurde – mit Verweis auf zwei Eurobarometer-Umfragen von 2008 – betont, dass die Bevölkerung sich der Gefahren unkontrollierter Datenverarbeitung durchaus bewusst sei, aber die Rechte in diesem Bereich kaum kenne, geschweige denn einfordere.

Vor dem Hintergrund dieser Ergebnisse hat die Grundrechteagentur nun eine vergleichende Studie zur Frage in Auftrag gegeben, wie den Menschen ihr Recht auf Datenschutz verschafft werden kann.[4] Mit Hinweis auf die Artikel 22 (Rechtsbehelfe), 23 (Haftung), 24 (Sanktionen) und 28 (Kontrollstelle) der EU-Datenschutzrichtlinie von 1995 stellt die Agentur fest, dass europaweit nur unzulängliche Informationen über den Zugang von Einzelpersonen zu rechtlichen und alternativen Formen der Wiedergutmachung in Datenschutzfragen verfügbar sind. Daher sollen in ausgewählten Ländern

die existierenden Rechtsbehelfe und Beschwerdemechanismen kartiert, Informationen zur Zahl der Beschwerden erhoben sowie Betroffene und Experten zu Erfahrungen und Zufriedenheit mit den bestehenden Möglichkeiten gehört werden.[5]

Beauftragt mit der Durchführung der nationalen Teilprojekte sind die „focal points“ des FRANET, eines 2011 ins Leben gerufenen Netzwerkes von Forschungseinrichtungen, die der Grundrechteagentur zuarbeiten. Deutscher „focal point“ des FRANET ist – in Kooperation mit dem Europäischen Forum für Migrationsstudien – das Deutsche Institut für Menschenrechte in Berlin, das 2001 auf Empfehlung des Bundestages gegründet wurde, um über die Lage der Menschenrechte in In- und Ausland zu informieren und zur Prävention von Menschenrechtsverletzung beizutragen.[6] Neben einer rechtlichen Bestandsaufnahme wird das Institut bis August 2012 Beschwerdeführer, aber auch Menschen, die sich trotz Verdachts auf Datenschutzverletzungen nicht gewehrt haben, zu ihren Motiven, Erfahrungen und Meinungen interviewen. Richter sollen zu Entscheidungen in Beschwerdeverfahren befragt werden, und Anwälte, Mitarbeiter aus Datenschutzbehörden sowie Vertreter von Nichtregierungsorganisationen werden gebeten, ihre Erfahrungen zu diskutieren.

Im Herbst werden schließlich die Forschungsergebnisse der nationalen Teilstudie ausgewertet und verglichen. Der abschließende Bericht soll 2013 erscheinen. Die Grundrechteagentur erhofft sich, mit den Ergebnissen der Studie den laufenden Gesetzgebungsprozess zur Datenschutznovelle zu informieren und durch die Identifizierung „guter Praktiken“ die Arbeit von Datenschutzbehörden und anderen Akteuren zu inspirieren. Man darf gespannt sein, ob z.B. der vermutlich nicht ohne Widerspruch bleibende Kommissionsvorschlag zur Einführung eines Verbandsbeschwerderechts (Art. 73, Abs. 2 und 3 des Vorschlags zur neuen Datenschutz-Grundverordnung)[7] durch die Studie argumentative Schützenhilfe erhält.

Der Autor ist Wissenschaftlicher Mitarbeiter des Deutschen Instituts für Menschenrechte und für die sozialwissenschaftliche Forschung im deutschen Teilprojekt der Studie zuständig. Falls Sie als betroffener (Nicht-)Beschwerdeführer, Richter, Anwalt, Mitarbeiter einer Aufsichtsbehörde oder einer Nichtregierungsorganisation Interesse haben, an der Studie teilzunehmen, kontaktieren Sie ihn bitte telefonisch unter 030-25.93.59.20 oder per Mail unter toepfer@institut-fuer-menschenrechte.de.

1 Beschluss des Rates (2008/203/EG) vom 28. Februar 2008 zur Durchführung der Verordnung (EG) Nr. 168/2007 hinsichtlich der Annahme eines Mehrjahresrahmens für die Agentur der Europäischen Union für Grundrechte für den Zeitraum 2007—2012. Amtsblatt der EU, L 63/14-15 v. 7.3.2008.

2 Verordnung (EG) Nr. 168/2007 des Rates vom 15. Februar 2007 zur Errichtung einer Agentur der Europäischen Union für Grundrechte. Amtsblatt der EU, L 53/1-14 v. 22.2.2007.

3 European Union Agency for Fundamental Rights: Data Protection in European Union: the Role of National Data Protection Authorities. Luxembourg 2010. Online unter: http://fra.europa.eu/fraWebsite/attachments/Data-protection_en.pdf

4 Geplant sind in 2012/13 daneben auch die Edition eines Handbuchs zum Fallrecht des europäischen Datenschutzes sowie eine Studie zum Datenschutzbewusstsein von Internetnutzern.

5 European Union Agency for Fundamental Rights: Annual Work Programme 2012. Vienna, S. 25. Online unter: http://fra.europa.eu/fraWebsite/attachments/FRA_AWP2012_EN.pdf

6 Ausführliche Informationen zum Institut auf der Website: www.institut-fuer-menschenrechte.de

7 Europäische Kommission: Vorschlag für Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung). KOM(2012) 11 endgültig v. 25.1.2012. Online unter: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_de.pdf

EDRI

Europäischer Datenschutz in der digitalen Gesellschaft

In Europa ist eine umfassende Reform des Datenschutzes mehr als überfällig. Seit der Richtlinie von 1995 führten der technische Fortschritt und die unterschiedliche Umsetzung in den Mitgliedstaaten dazu, dass wir heute dringend eine Novellierung und einheitliche europäische Datenschutzgesetze brauchen. Angesichts der immer zentraler werdenden Rolle des Internet und der wachsenden globalen Vernetzung setzt sich European Digital Rights (EDRi) dafür ein, dass Datenschutz heutzutage nicht mehr an Staatsgrenzen aufhört.

Die aktuellen Probleme im Kampf für besseren Datenschutz in Europa lassen sich anhand von „Facebook vs. Europe“ gut veranschaulichen. Im letzten Jahr erstattete ein österreichischer Student bei der irischen Datenschutzbehörde insgesamt 22 Anzeigen gegen Facebook und forderte sämtliche über ihn gespeicherte Daten an. Da Facebook seinen Sitz in Dublin hat, sind europäische Facebook-Nutzer derzeit durch den Nutzungsvertrag von der irischen Gesetzgebung abhängig. Einheitliche Datenschutzgesetze sind notwendig, denn Nutzer sozialer Netzwerke sollten endlich über ein ausreichendes Schutzniveau verfügen – auch wenn Unternehmen ihren Sitz in einem anderen Mitgliedstaat haben.



Dies wirft direkt eine weitere Frage auf: Wie kann, bei einem steigenden Grad der globalen Vernetzung, mit der extraterritorialen Rechtsanwendung durch Drittländer umgegangen werden? Die USA wenden beispielsweise seit einigen Jahren den PATRIOT Act sowie den Foreign Intelligence Surveillance Act (FISA) an, um auf Daten ausländischer Personen zugreifen zu können, die in keiner Verbindung zu den USA stehen. Es ist essentiell, dieses rechtliche Vakuum endlich mit einer umfassenden Datenschutzreform zu beenden – die gegenwärtigen Beschränkungen sind de facto wirkungslos. Die neue Datenschutzverordnung muss dazu beitragen, den unkontrollierten Transfer personenbezogener Daten europäischer Bürger in Drittländer einzudämmen. Auch die neue Richtlinie für den Bereich Polizei und Justiz sollte strengere Regeln für den Zugriff von Ermittlungsbehörden in anderen EU-Ländern auf personenbezogene Daten aufstellen.

Weiterhin bestehen derzeit Probleme der Regulierung durch Staaten einerseits und Selbstregulierungsversuche durch Unternehmen zum angeblichen Schutz der Nutzer anderseits. Aufgrund der Anzeigen wurde Facebook von der irischen Datenschutzbehörde geprüft und musste bereits die Anschuldigung des laschen Vorgehens über sich ergehen lassen – ohne Gefahr zu laufen, sanktioniert zu werden. Die Untersuchungsberichte wurden dort sogar nur im Einvernehmen mit dem US-Unternehmen veröffentlicht.

Zum anderen fordert die Wirtschaft seit längerem die Einführung unternehmensinterner Datenschutzregelungen und des sogenannten Grundsatzes der Rechenschaftspflicht. Aus dem Blickwinkel einer effizienteren Umsetzung von Datenschutzgesetzen erscheint dieser Ansatz zunächst begrüßenswert – allerdings darf dies unter keinen Umständen zu einer Lockerung der Verpflichtungen führen und muss vor allem auch für den Bereich der internationalen Datenübertragung gelten, wie die Artikel 29 Datenschutzgruppe bereits in einer Stellungnahme von 2010 forderte.

Dann gibt es noch die zahlreichen Gesetzeslücken, die dringend gefüllt werden müssen. Viele Unternehmen erlauben sich durch ihre Allgemeinen Geschäftsbedingungen, die Daten der Nutzer frei zu verwenden und ändern die AGBs, wann immer sie möchten. Der Online-Speicherdienst Dropbox änderte beispielsweise im letzten Jahr mehrere Male die Nutzungsbedingungen. Im April 2011 kam eine Klausel dazu, mit der Nutzer einwilligten, dass US-Behörden auf Anfrage Zugriff auf ihre Daten bekommen. In der Regel gilt, dass – jedenfalls solange diese Fälle nicht in der Presse bekannt werden - Nutzer meistens unbewusst ihre Rechte abgeben.

Die Vorschläge der EU-Kommission für eine allgemeine Datenschutzreform sind daher wichtig und notwendig. Gleichzeitig muss aber eine effektive Implementierung sichergestellt werden. Dies kann zum Beispiel durch die Einführung von obligatorischen Datenschutz-Folgenabschätzungen gewährleistet werden. Wirklich unabhängige und angemessen ausgestattete Datenschutzbehörden sind ebenfalls eine Voraussetzung für eine Umsetzung der Regeln in die Praxis. Auch müssen datenschutzfreundliche Voreinstellungen für europäische Politikgestaltung gelten, wie bei der Ausarbeitung von Richtlinien wie z.B. zur Vorratsdaten- oder Fluggastdatenspeicherung in Europa.

Angesichts der zahlreichen Baustellen haben Datenschützer auf europäischer Ebene im Moment reichlich viel zu tun. Als Vernetzungsknoten für nationale Bürgerrechts- und Datenschutzorganisationen sorgt EDRi in Brüssel dafür, dass bei der Politikgestaltung die Interessen der Bürger und die EU-Grundrechtecharta nicht nur berücksichtigt, sondern konsequent zur Bedingung werden.

Das Büro in Brüssel ist seit September 2011 auf drei Leute angewachsen und versucht, dort ein Gegengewicht zu den über 15.000 Industrie-Lobbyisten herzustellen. EDRi ist ein Zusammenschluss von 28 Bürgerrechts- und Datenschutzorganisationen (FoeBuD, CCC, Vibe!At, Bits of Freedom, Open Rights Group...) aus insgesamt 18 verschiedenen europäischen Ländern. Damit ist EDRi die (bisher) einzige Brüsseler Stimme der Zivilgesellschaft für alle datenschutzrechtlichen und netzpolitischen Aspekte in der digitalen Gesellschaft.

Kontakt:
European Digital Rights
Rue Montoyer 39/9
B-1000 Brussels
http://edri.org

Hinweis der Redaktion:
Die Deutsche Vereinigung für Datenschutz wird im Jahr 2012 ihre Mitgliedschaft beantragen.

Cornelia Ernst, MdEP, und Lorenz Krämer

Die Reform des europäischen Datenschutzrechts im Parlament

Am 25. Januar hat die Europäische Kommission ihre lange erwarteten Vorschläge zum Ausbau des europäischen Datenschutzes vorgelegt. Die Vorschläge basieren auf dem mit dem Lissabon-Vertrag neu geschaffenen Artikel 16, mit dem die EU eine eigenständige Kompetenz für den Datenschutz erhalten hat. Gleichzeitig wurde die Europäische Grundrechtecharta Teil der Verträge: EU-Recht muss damit in Zukunft dem dort in Artikel 8 festgelegten Recht auf Datenschutz genügen.

Das Europaparlament hatte schon im Juni 2011 im Voss-Bericht mit breiter, überparteilicher Mehrheit eine Reihe Anforderungen für die anstehende Reform des Datenschutzes formuliert, von denen sich viele, aber längst nicht alle, in den nun vorliegenden Vorschlägen wiederfinden. Es wurde klar gestellt, dass das Parlament eine Erneuerung der Datenschutzrichtlinie 95/46/EG begrüße, solange diese auf den Prinzipien der bisher geltenden Regelung beruhe und auf keinen Fall dahinter zurückfallen dürfe. Weitere Forderungen waren unter anderem, dass in Zukunft der Datenschutz in den Mitgliedstaaten soweit als möglich harmonisiert werden sollte, dass die Verarbeitung persönlicher Daten auf einer expliziten und informierten Einwilligung beruhen müssten und die bestehenden Regeln daher präzisiert werden sollten, dass *privacy by default* und *privacy by design* als neue Grundsätze aufgenommen werden sollten und dass bei Verstößen wirkungsvolle Sanktionen vorgesehen sein müssten. Diese Forderungen finden sich in dem Vorschlag für die allgemeine Datenschutz-Grundverordnung im Großen und Ganzen wieder.

Andere, durchaus zentrale Anliegen des Parlaments finden sich dagegen nicht wieder. Dazu gehört die Forderung nach einer Regelung aus einem Guss, die den Datenschutz in allen Bereichen betrifft. Auf dem Tisch liegen nun aber zwei Vorschläge. Der Datenschutz im Bereich der Strafverfolgung ist Gegenstand eines separaten Richtlinienvorschlags, den der Europäische Datenschutzbeauftragte Peter Hustinx wegen des geringen Schutzniveaus schlicht als „unangemessen“ bezeichnet hat. Das ist besonders bedenklich, handelt es sich doch um einen Bereich, der naturgemäß tiefgreifende Folgen für die Betroffenen haben kann.

Von beiden Legislativvorschlägen unberührt bleibt die Datenverarbeitung durch Organe und Institutionen der EU, ebenso im Widerspruch zu den Forderungen des Parlaments. Derzeit wird dieser Bereich durch die Verordnung 45/2001 geregelt, deren Reformbedürftigkeit durchaus unbestritten ist. Es ist auch schwer einzusehen, warum die Datenverarbeitung, die etwa von Behörden in den Mitgliedstaaten durchgeführt wird, unter den Wirkungsbereich der neuen Verordnung fallen soll, die Datenverarbeitung durch die verschiedenen EU-Agenturen dagegen nicht. Das gilt umso mehr, wenn man bedenkt, dass die EU nicht nur als Arbeitgeber mehrer Zehntausend Beamter und Angestellter fungiert, sondern in der Mehrzahl der Fälle auch als deren Kranken- und Sozialversicherung. Daneben darf auch nicht vergessen werden, dass zum Beispiel mit FRONTEX oder Europol auch EU-Agenturen bestehen, deren Aktivitäten zumindest teilweise im Bereich der Strafverfolgung oder Kriminalitätsprävention liegen und die ihre gespeicherten Daten auch untereinander austauschen.

Bei allen Schwächen der beiden Vorschläge hilft es indes nicht, auf Nachbesserungen durch die Kommission zu hoffen. Der Ball liegt jetzt ganz klar beim Europaparlament, wo sich nun der Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres mit den Vorlagen befassen wird. Die beiden Berichte, die der Ausschuss dann verfasst, werden im Wesentlichen eine abgeänderte Fassung der Texte enthalten, die über Änderungsanträge und Kompromissverhandlungen im Prinzip gemeinsam erarbeitet wird. Nach dieser Phase stünde dann eigentlich die Abstimmung im Ausschuss mit folgender Abstimmung im Plenum an, womit das Parlament seine erste Lesung abschließen würde. Die resultierende Fassung des Textes könnte der Rat dann akzeptieren, womit die Verordnung angenommen wäre, oder eine eigene, abweichende Position beschließen, was eine zweite Lesung notwendig machen würde.

Wahrscheinlicher ist es aber, dass ein anderes Prozedere zum Tragen kommt. Statt einer endgültigen Abstimmung wird der Innenausschuss eher nur eine vorläufige „Probeabstimmung“ abhalten. Auf Grundlage der resultierenden „vorläufigen“ Textfassung wird dann der sogenannte „Trilog“ eingeleitet, dabei handelt es sich um Dreiecksverhandlungen, bei denen neben Parlamentsvertretern Vertreter von Kommission und Ministerrat an einem Tisch sitzen. Der Rat wird vorher ebenso wie das Parlament eine eigene Wunschversion der Texte erarbeitet haben. Gelingt es dann, sich in diesem Trilog auf eine gemeinsame Version zu einigen, kann auf dieser Grundlage der Ausschuss dann seine eigentliche Abstimmung nachholen, Parlamentsplenum und Rat dieselbe ausgehandelte Fassung beschließen und das Verfahren folglich noch in der ersten Lesung abschließen. Vorausgesetzt, dass sowohl das Parlament als auch der Rat ein Interesse an einer Neuregelung des Datenschutzes haben, können wir davon ausgehen, dass diese Verhandlungen irgendwann zu einem erfolgreichen Abschluss führen werden.

Es ist klar, dass dieser Vorgang einige Zeit in Anspruch nehmen wird.

Insbesondere in den entscheidenden Phasen, nämlich wenn die Fraktionen im Innenausschuss untereinander Kompromisse verhandeln werden und dann wieder während des Trilogs, wird übermäßige Eile sicher keine Vorteile bringen. Die Vorschläge sind von viel zu weitreichender Tragweite, um ohne Not irgendwelche Positionen aufzugeben, nur damit die Verhandlungen schneller abgeschlossen werden. Für den Fall, dass die Verhandlungen einmal wegen anscheinend unüberbrückbarer Differenzen stecken bleiben sollten, gilt zu bedenken: Das Europaparlament wird alle fünf Jahre neu gewählt, die Mehrheiten im Rat dagegen sind bei weitem nicht so konstant.

Alexander Dix

Vorratsdatenspeicherung widerspricht europäischen Grundrechten[1]

Als das **Bundesverfassungsgericht** am 2. März 2010 die Regelungen zur anlassunabhängigen Speicherung von Telekommunikationsverkehrsdaten mit sofortiger Wirkung für verfassungswidrig erklärte, war das für manche Politiker ein Schock. Der frühere Berliner Innensenator Körting wies dagegen darauf hin, dass das Gericht die Vorratsdatenspeicherung nicht prinzipiell für verfassungswidrig erklärt habe; vielmehr habe es dem Gesetzgeber so präzise Vorgaben gemacht, dass jetzt jeder **Rechtsreferendar** in der Lage wäre, ein verfassungskonformes Gesetz zur Vorratsspeicherung zu entwerfen.

Trotzdem ist bisher kein solches Gesetz in Deutschland verabschiedet worden, und das aus gutem Grund. Denn auch nach der Entscheidung des Bundesverfassungsgerichts und nach dem Inkrafttreten der europäischen Richtlinie zur Vorratsdatenspeicherung 2006/24 muss die Frage gestellt werden, *ob* wir die Vorratsdatenspeicherung in Europa einführen können/wollen, und nicht nur, *wie* dies zu bewerkstelligen ist.

Rechtliche Maßstäbe

Die Antwort auf diese Grundfrage hängt davon ab, ob die Richtlinie von 2006 mit der **Europäischen Grundrechte-Charta** und der **Europäischen Menschenrechtskonvention** vereinbar ist. Diese Frage haben weder das Bundesverfassungsgericht noch der Gerichtshof der Europäischen Union in Luxemburg noch der Europäische Gerichtshof für Menschenrechte in Straßburg beantwortet. Das Bundesverfassungsgericht ist dieser Frage ausgewichen, weil es offenbar den Konflikt mit dem EuGH scheute (auf das gleichwohl wichtige Urteil vom 2.3.2010 komme ich noch zurück). Der Berichterstatter im 1. Senat, Johannes Masing, hat kürzlich in der *Süddeutschen Zeitung* die Gefahr heraufbeschworen, dass durch eine künftige Europäische Datenschutzverordnung der deutsche Grundrechtsschutz und die Stellung des Bundesverfassungsgerichts ausgehöhlt werden könnte. Diese Gefahr besteht nicht erst bei Verabschiedung einer Datenschutzverordnung, sie bestand schon früher, etwa bei der Verabschiedung der Vorratsdatenrichtlinie. Denn auch eine Richtlinie hat Vorrang vor den Grundrechtsgarantien des Grundgesetzes. Weder die Bundesregierung noch das Bundesverfassungsgericht (das das Recht auf informationelle Selbstbestimmung 1983 erfunden und die Bedeutung dieses Rechts bis heute immer wieder hervorgehoben hat) sind dieser Gefahr der Aushöhlung von Grundrechten durch das Unionsrecht zur Vorratsdatenspeicherung entschieden genug entgegengetreten.

Der **EuGH** selbst hat zwar schon drei Mitgliedstaaten (Griechenland, Schweden und Österreich) wegen unterlassener Umsetzung der Vorratsdatenrichtlinie verurteilt (ohne bisher Sanktionen zu verhängen), dabei ist er aber nicht darauf eingegangen, ob diese Richtlinie gegen Unionsgrundrechte verstößt. Formal hatte er dazu auch keine Veranlassung, weil die Mitgliedstaaten auch solche Richtlinien umsetzen müssen, die gegen Grundrechte verstoßen, wenn sie es versäumt haben, rechtzeitig die Nichtigkeit der Richtlinie feststellen zu lassen (schwer erträglich). Auch betroffene Bürger hätten eine solche Nichtigkeitsklage gegen die Richtlinie erheben können, haben dies aber nicht innerhalb der vom Unionsrecht vorgegebenen Zweimonatsfrist getan hat. Soeben hat allerdings der irische High Court seine schon vor zwei Jahren gemachte Ankündigung wahr gemacht und die Frage der Vereinbarkeit der Vorratsdatenrichtlinie mit der Europäischen Grundrechte-Charta dem EuGH zur Entscheidung vorgelegt[2].

Der **Europäische Gerichtshof für Menschenrechte** wiederum konnte über die Frage noch nicht entscheiden, weil er meines Wissens noch nicht angerufen wurde. Die Menschenrechtskonvention hat zwar in Deutschland nur den Rang eines einfachen Gesetzes. Dennoch dürfte ihre Bedeutung deutlich zunehmen, wenn die Europäische Union – wie es der Vertrag von Lissabon (Art. 6 Abs.2 EUV) vorsieht – der Konvention beitritt, und damit auch Rechtsakte der Union vom Menschenrechtsgerichtshof kontrolliert werden können. Schon jetzt sind nach diesem Vertrag die Grundrechte, wie sie in der Menschenrechtskonvention gewährleistet sind und wie sie sich aus den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten ergeben, als allgemeine Grundsätze Teil des Unionsrechts (Art. 6 Abs. 3 EUV).

Ich erinnere daran, dass der Europäische Menschenrechtsgerichtshof gerade in letzter Zeit wiederholt – etwa beim Persönlichkeitsrechtsschutz und bei der Sicherungsverwahrung – die Rechtsprechung des Bundesverfassungsgerichts korrigiert hat.

Artikel 8 der Menschenrechtskonvention garantiert jeder Person das Recht auf Achtung ihres Privatlebens und zählt dazu auch die „Korrespondenz". **Artikel 7 der Europäischen Grundrechte-Charta** ist nahezu wortgleich formuliert, spricht aber zeitgemäßer von „Kommunikation". Damit sind wie beim Fernmeldegeheimnis nicht nur der Inhalt der Kommunikation, sondern auch ihre Begleitumstände gemeint, also wer mit wem von wo aus kommuniziert hat. Gerade diese Begleitumstände sollen nach der Vorratsdaten-Richtlinie anlassunabhängig und ohne Verdachtsmomente mindestens für ein halbes Jahr gespeichert werden.

Auch die Europäische Menschenrechtskonvention lässt allerdings Eingriffe in den Schutz des Privatlebens und der Kommunikation ausnahmsweise dann zu, wenn sie **„in einer demokratischen Gesellschaft notwendig**" für bestimmte Zwecke sind. Der Europäische Gerichtshof für Menschenrechte hat diese Formulierung stets sehr restriktiv im Sinne eines „dringenden gesellschaftlichen Bedürfnisses" (*pressing social need*) interpretiert; zudem müssten einschränkende Maßnahmen verhältnismäßig bezogen auf das verfolgte Ziel sein. In seiner Abhörentscheidung (Fall Klass u.a. gegen Deutschland) hat der Gerichtshof 1978 formuliert:

„Gleichwohl unterstreicht der Gerichtshof, dass dies nicht bedeutet, die Vertragsstaaten hätten ein unbegrenztes Ermessen, Personen innerhalb ihres Hoheitsbereichs geheimer Überwachung zu unterwerfen. Im Bewusstsein der Gefahr, die ein solches Gesetz in sich birgt, nämlich die Demokratie mit der Begründung, sie zu verteidigen, zu untergraben oder sogar zu zerstören, bekräftigt der Gerichtshof, dass die Vertragsstaaten nicht im Namen des Kampfes gegen Spionage und Terrorismus zu jedweder Maßnahme greifen dürfen, die ihnen *geeignet* erscheint."

Zwar ging es im Fall Klass – anders als bei der Vorratsdatenspeicherung – um eine heimliche Überwachung der Kommunikations*inhalte* durch Abhörmaßnahmen der Nachrichtendienste. Das Bundesverfassungsgericht hat aber betont, dass der Rückgriff auf Verkehrs- (Rand- oder Meta-) daten der Telekommunikation nicht weniger schwer wiegt als eine Überwachung der Telekommunikationsinhalte. Denn sie erlauben tief in das Privatleben eindringende Rückschlüsse und ermöglichen unter Umständen detaillierte Persönlichkeits- und Bewegungsprofile. Andererseits waren und sind Abhörmaßnahmen nur bei Vorliegen bestimmter Voraussetzungen im Einzelfall zulässig, nicht aber routinemäßig und auf Vorrat.

Die Vereinbarkeit der Vorratsdaten-Richtlinie mit der Europäischen Menschenrechtskonvention und damit auch der Grundrechte-Charta der Europäischen Union hängt deshalb von der Frage ab, ob eine verdachtsunabhängige, anlasslose Speicherung sämtlicher Telekommunikationsverkehrsdaten in einer demokratischen Gesellschaft zwingend notwendig ist. Auf ihre – unbestrittene – **Nützlichkeit** für die Kriminalitätsbekämpfung (die niemand bestreitet) kommt es in diesem Zusammenhang auch nach Auffassung des Bundesverfassungsgerichts nicht an, sie rechtfertigt keine so weitreichenden Eingriffe in die Grundrechte.

Zwingend notwendig in einer demokratischen Gesellschaft?

Die verdachtsunabhängige Speicherung aller Telekommunikationsverkehrsdaten ist in einer demokratischen Gesellschaft nicht zwingend notwendig. Darüber hinaus birgt sie auch **neue, zusätzliche Sicherheitsrisiken**.

Dass die Vorratsdatenspeicherung keine notwendige Voraussetzung für die Bekämpfung schwerer Straftaten wie Terrorismus und organisierter Kriminalität ist, hätte dem europäischen Gesetzgeber schon bei Verabschiedung der Richtlinie von 2006 klar sein müssen: die überlebenden Urheber sowohl der Terroranschläge in London als auch in Madrid wurden zur Rechenschaft gezogen, obwohl es in beiden Staaten damals noch keine Vorratsspeicherpflicht gab. Es gibt zum einen gegenwärtig **keine öffentlich überprüfbaren Belege** dafür, dass die Bekämpfung von Straftaten seit dem 2. März 2010 erkennbar erschwert worden wäre[3]. Wenig überzeugend sind auch aktuelle Versuche, die Bekämpfung des Rechtsterrorismus als Beleg für die Notwendigkeit der Vorratsdatenspeicherung anzuführen.

Geradezu grotesk mutet es an, wenn vereinzelt sogar das Fehlen der Vorratsspeicherung als Erklärung oder Entschuldigung für das Versagen der Sicherheitsbehörden bei der Verfolgung des „Nationalsozialistischen Untergrunds" herangezogen wird. Wenn Verfassungsschutz und Polizei zehn Jahre lang zahlreiche Morde aus Gründen nicht aufklären können, die noch zu beleuchten sein werden, dann hätte eine sechsmonatige Speicherung von Telekommunikationsverkehrsdaten nichts genutzt. Wenn aber die Vorratsspeicherung solcher Daten generell als Mittel zur Reparatur von Versäumnissen der Sicherheitsbehörden in einer wie lange auch immer zurückliegenden Vergangenheit herhalten sollen, dann müssten alle Verkehrsdaten **unbefristet** gespeichert werden. Noch ist ein solcher Vorschlag nicht gemacht worden.

Schließlich hat auch die **Europäische Kommission** selbst offenbar mittlerweile **Zweifel**, ob die Vorratsspeicherung zwingend notwendig ist. Im Rahmen der laufenden Konsultation zur Reform der Vorratsdaten-Richtlinie hat sie in ihrem Bericht vom Dezember 2011 festgestellt, dass es nach wie vor kaum belastbare Nachweise für die Notwendigkeit der Vorratsspeicherung gibt. Die Mitgliedstaaten würden lediglich die Wichtigkeit dieser Daten verbal betonen, ohne **Alternativen wie das Quick-Freeze-Verfahren** zu prüfen. **Nur 11 von 27 Mitgliedstaaten** hätten Daten geliefert, die einen Mehrwert der Vorratsdatenspeicherung nahelegten. Auch sei unklar, ob Verkehrsdaten nicht auch ohne Pflicht zur Bevorratung in ausreichendem Umfang vorhanden seien. Zuletzt gab es auch in Deutschland Hinweise darauf, dass Netzbetreiber schon gegenwärtig Verkehrsdaten länger vorhalten als für Abrechnungszwecke erforderlich. Dem geht gegenwärtig die **Bundesnetzagentur** nach. Die Kommission kritisiert, dass es keine Übersicht darüber gebe, welchen Effekt genutzte Verkehrsdaten in Ermittlungen

und Verfahren gehabt hätten. Der Katalog der Straftaten werde in den Mitgliedstaaten uneinheitlich umgesetzt und es gebe bereits Forderungen, die Vorratsdaten auch zur Verfolgung von Urheberrechtsverstößen nutzbar zu machen.

Die deutschen Sicherheitsbehörden (hier: das Bundeskriminalamt) haben in einer Auflistung der Beispielsfälle, in denen Mindestspeicherfristen notwendig wären, auch **Trickbetrügereien am Telefon** genannt. Hier wird die Gefahr der schleichenden Zweckentfremdung, des *function creep*, deutlich. Diese Gefahr ist – wie der neueste Kommissionsbericht belegt – nicht gebannt. Der ursprüngliche Anlass für den europäischen Gesetzgeber, nämlich terroristische Anschläge, gerät damit ebenso aus dem Blick wie die Aussage des Bundesverfassungsgerichts, das eine Zweckentfremdung der Vorratsdaten ausschließen wollte. Aber selbst das Verfassungsgericht hat die Nutzung von auf Vorrat gespeicherten IP-Adressen zur Verfolgung gewichtiger Ordnungswidrigkeiten für verfassungskonform gehalten.

Die EU-Kommission hat angekündigt, **bis Juli 2012 einen Vorschlag für eine geänderte Vorratsdaten-Richtlinie** vorzulegen, der auch grundrechtsschonendere Alternativen berücksichtigen soll. Ich halte es für unwahrscheinlich, dass die Kommission vor diesem Zeitpunkt gegen die Mitgliedstaaten Sanktionen beantragen wird, die die alte Richtlinie noch nicht umgesetzt haben. Es würde dem Rechtsgrundsatz des *venire contra factum proprium* widersprechen.

Diese Feststellungen zeigen aber zugleich, dass die gegenwärtige Richtlinie nicht die engen Voraussetzungen der Europäischen Menschenrechtskonvention für Eingriffe in das Kommunikationsgeheimnis erfüllt: die anlassunabhängige Speicherung der Verkehrsdaten ist nicht zwingend erforderlich in einer demokratischen Gesellschaft.

Deshalb ist die Bundesregierung gut beraten, keinen Vorschlag zur Umsetzung der nicht grundrechtskonformen Vorratsdaten-Richtlinie zu machen, zumindest aber den Vorschlag der Kommission für eine geänderte Richtlinie abzuwarten. Diese Auffassung wird auch durch eine Entscheidung des EGMR aus dem Jahr 2008 gestützt. Darin hat der Gerichtshof die Befugnis britischer Behörden beanstandet, pauschal und unterschiedslos Fingerabdrücke, Zellproben und DNA-Profile von verdächtigen, aber noch keiner Straftat schuldig gesprochenen Personen aufzubewahren. Wenn eine solche undifferenzierte Befugnis zur Sammlung von Daten schon bei *verdächtigen* Personen der Menschenrechtskonvention widerspricht, gilt dies erst recht bei Telekommunikationsteilnehmern, die in der großen Mehrzahl *unverdächtig* sind.

Neue Sicherheitsrisiken durch Vorratsspeicherung

Die Vorratsdatenspeicherung widerspricht aber nicht nur europäischen Grundrechtsstandards, sie führt auch zu neuen Sicherheitsrisiken. In der mündlichen Verhandlung zur Vorratsdatenspeicherung beim Bundesverfassungsgericht hat der zu früh verstorbene Andreas Pfitzmann dies anschaulich verdeutlicht, indem er eine daumennagelgroße **Micro-SD-Speicherkarte** im Wasserglas des anwesenden BKA-Präsidenten versenkte. Er wollte damit dem Gericht verdeutlichen, dass die bei der Vorratsspeicherung entstehenden riesigen Mengen an Verkehrsdaten sich auch mit noch so großem Aufwand nicht zuverlässig gegen unberechtigte Zugriffe sichern lassen. Ein Insider kann große Mengen solcher Daten auf kleine Speichermedien kopieren, um sie zu verschlucken und unerkannt aus Rechenzentrum eines Providers herausbringen. Solche Speichermedien sind nicht nur wasserfest, sondern auch unempfindlich gegen Magensäure. Dieses Beispiel mag skurril anmuten, aber es illustriert, dass eine Verpflichtung zur Speicherung sämtlicher Verkehrsdaten für einen bestimmten Zeitraum **unkontrollierbare Risiken für die Datensicherheit** auslösen würde, die bisher nicht bestanden. Während der Sicherheitsgewinn durch Vorratsspeicherung mehr als zweifelhaft ist, müssen solche Risiken ernst genommen werden. Denn nicht jeder Hacker hat so ehrenwerte Motive wie der Chaos Computer Club bei der Enttarnung des Staatstrojaners.

Ich will noch auf eine andere, weitergehende Gefahr hinweisen, die die Vorratsdatenspeicherung birgt: Wenn auf Anweisung des Staates sämtliche Verkehrsdaten zur Telekommunikation jedes Menschen für einen bestimmten Zeitraum (ganz gleich wie lang) auf Vorrat gespeichert wird, um terroristische oder andere Straftaten besser bekämpfen zu können, dann wird in der Bevölkerung die Illusion genährt, jetzt vor solchen Straftaten endgültig sicher zu sein. In dem wahrscheinlichen Fall, dass diese Erwartung enttäuscht wird und auch durch die Vorratsdatenspeicherung Terroranschläge nicht verhindert werden können (z.B. weil die Sicherheitsbehörden in dem Heuhaufen von Millionen Verkehrsdatensätzen den entscheidenden Hinweis, die „Nadel" nicht rechtzeitig finden, dann droht eine tiefe Legitimationskrise der Sicherheitsbehörden und des Staates insgesamt, weil die Menschen wissen wollen, warum die Vorratsdatenspeicherung, die so lange als Wunderwaffe angepriesen wurde, nicht genützt hat.

Überwachungsgesamtrechnung

Schließlich ist an eine Schlüsselpassage in dem Urteil des Bundesverfassungsgerichts vom 2. März 2010 zu erinnern, in der das Gericht wörtlich ausführt:

„Die Einführung der Telekommunikationsverkehrsdatenspeicherung kann damit nicht als Vorbild für die Schaffung weiterer vorsorglich anlassloser Datensammlungen dienen, sondern zwingt den Gesetzgeber bei der Erwägung neuer Speicherungspflichten oder – berechtigungen im Blick auf die **Gesamtheit der verschiedenen schon vorhandenen Datensammlungen** zu größerer Zurückhaltung. **Dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf, gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland, für deren Wahrung sich die Bundesrepublik in europäischen und internationalen Zusammenhängen einsetzen muss.** Durch eine vorsorgliche Speicherung der Telekommunikationsverkehrsdaten wird der Spielraum für weitere anlasslose Datensammlungen auch über den

Weg der Europäischen Union erheblich geringer (Rz. 218).“

Mit dem Topos der „Überwachungsgesamtrechnung“ hat das Bundesverfassungsgericht eine **rote Linie** formuliert, ohne allerdings genau zu sagen, wann sie überschritten wird. Zweierlei wird man aber sagen können:

Zum einen muss sich die Bundesregierung, wenn sie die bisherige Vorratsdatenrichtlinie in nationales Recht umsetzen wollte, auch auf europäischer Ebene gegen weitere Vorhaben zur anlassunabhängigen Datenspeicherung aussprechen. Es reicht deshalb nicht aus, dass der Bundesinnenminister sich im Europäischen Rat der Stimme enthält, wenn über den Vorschlag der Kommission über eine Speicherung und Übermittlung von Fluggastdaten auf Vorrat in die USA abgestimmt wird. Er war verfassungsrechtlich verpflichtet, gegen eine solche Maßnahme zu stimmen. Ob dieser Vorschlag die notwendige Zustimmung des Europäischen Parlaments finden wird, ist gegenwärtig offen.

Zum anderen gilt: Wenn der europäische Gesetzgeber die Fluggastdatenspeicherung anordnet, ohne im Bereich der Telekommunikationsverkehrsdaten den Mitgliedstaaten mehr Spielraum (z.B. für Quick Freeze) zu eröffnen, dann spätestens ist die rote Linie endgültig überschritten, die das Bundesverfassungsgericht beschrieben hat. Aber selbst wenn das Europäische Parlament, was zu wünschen wäre, der Fluggastdatenspeicherung eine Absage erteilen würde, muss auch die anlassunabhängige Speicherung von Telekommunikationsverkehrsdaten unterbleiben. Ein **Kompensationsgeschäft** darf es nicht geben.

Der frühere, für Inneres und Justiz zuständige EU-Kommissar **Frattini** (später Außenminister im Kabinett Berlusconi) sagte in einem Interview 2008, er sei „verrückt nach Sicherheit.“[3] Ich hoffe sehr, dass sowohl auf europäischer wie auch auf deutscher Ebene jetzt wieder Besonnenheit und Augenmaß Einzug halten, wenn es um die Balance zwischen Freiheit und Sicherheit geht.

1 Überarbeitete Fassung des beim 6. Europäischen Datenschutztag am 27.1.2012 in Berlin gehaltenen Impulsreferats

2 Vgl. http://heise.de/newsticker/meldung/Vorratsdatenspeicherung-vs-Grundrechte-1424117.html

3 Das ergibt sich auch aus dem Gutachten des Max-Planck-Instituts für ausländisches und internationales Strafrecht „Keine Schutzlücken durch Wegfall der Vorratsdatenspeicherung“ v. 27.1.2012

4 Der Spiegel 11/2008 v. 10.3.2008

Thilo Weichert

Verantwortlichkeit für Facebook-Fanpages

Zugleich eine parteiische Besprechung von Schulz/Schliesky (Hrsg.), Transparenz, Partizipation, Kollaboration – Web 2.0 für die öffentliche Verwaltung, 2012.

I. Verzweiflung

Für jemanden, für den Datenschutz, demokratische Verantwortlichkeit und Rechtsstaatlichkeit ein Anliegen ist, ist die Situation fast zum Verzweifeln: Da verstößt der US-Anbieter des weltweit größten Sozialen Netzwerks gegen gesetzliche Regelungen des europäischen und deutschen Datenschutzes, und es scheint gegen dessen Nutzung in Deutschland kein rechtliches Kraut gewachsen zu sein. Wir reden hier über Facebook und die Nutzung von seinen Fanpages sowie Social Plugins wie z. B. dem „Gefällt mir“-Button. Facebook ist exemplarisch für die Verzweiflung; viele andere Anbieter, allen voran Google+, sind nicht viel besser; deutsche Anbieter, die sich bemühen, die Datenschutzbestimmungen zu beachten, werden vom Markt verdrängt.

II. Politisch-wirtschaftliche Erwägungen

Diese Verzweiflung wird dadurch gesteigert, dass fast alle politischen Kräfte gegen diesen massiven fortgesetzten Rechtsverstoß nichts unternehmen und dass private Anbieter in realistischer Abwägung der Möglichkeiten und Risiken von der Nutzung dieser Fanpages und Social Plugins nicht ablassen[1]. Dass viele politische Kräfte nichts unternehmen, mag dem Umstand zuzuschreiben sein, dass viele der Menschen, Parteien und Organisationen in der Politik zwecks potenziellen Erreichens einer jugendlichen Wählerschaft solche Fanpages selbst betreiben. Dass private Anbieter selbst in Schleswig-Holstein sich bei der Nutzung von Facebook, Google+ & Co. recht entspannt zurücklehnen, ist der realistischen Einschätzung zuzuschreiben, dass das ULD noch etwas anderes zu tun hat, als hunderte Untersagungsverfügungen zu versenden[2]. Dies wird auch von den Regierungsfraktionen des Landes kommuniziert in der wohl irrigen Annahme, damit den Wirtschaftsstandort zwischen den Meeren zu verteidigen[3].

Nicht nur die Parlamentarier einiger Parteien verhalten sich abweisend gegenüber dem ULD-Vorgehen gegen die Facebook-Nutzung. Die Unwilligkeit, Datenschutzregeln zu beachten wird dadurch gefördert, dass die eigene Industrie- und Handelskammer (IHK) und der eigene Ministerpräsident selbst den Rechtsverstoß begehen. Nun werden keine IHK und kein deutscher Ministerpräsident öffentlich und explizit zum Rechtsverstoß aufrufen oder ermuntern. Sie wollen auch nicht als schlechtes Beispiel und Vorbild vor-

angehen. Deshalb wird eine – bisher eher unjuristisch vorgetragene – Argumentation präsentiert, die letztlich diesen Rechtsverstoß decken soll: Dass der US-Anbieter gegen deutsches Recht verstößt, ist zwar evident, doch wäre es vermessen, von einem globalen Player zu erwarten, dass er schleswig-holsteinisches Recht beachtet (selbst wenn er Daten von Schleswig-Holsteinern verarbeitet). Weiter wird vorgetragen: Wir sind nicht für das verantwortlich, was der US-Anbieter macht, wir nutzen nur dessen Angebot. Und letztlich: Dass wir das Angebot nutzen, kann uns niemand vorwerfen, machen es doch viele andere auch. Besser noch: Das Verbieten des Nutzens eines illegalen Angebots wäre – und das ist in einer Marktwirtschaft ein schwerwiegender Vorwurf – eine Wettbewerbsverzerrung.

III. Die juristische Argumentation

Die Diskussion um Facebook in Schleswig-Holstein bringt uns eine juristische Überhöhung dieser wirtschaftlich-politischen Argumente. Das Glanzstück liefert insofern jetzt das Lorenz-von-Stein-Institut der Christian-Albrechts-Universität zu Kiel (CAU) mit seinem neuen Buch „Transparenz, Partizipation, Kollaboration – Web 2.0 für die öffentliche Verwaltung“[4]. In einer gemeinsamen Medieninformation der CAU mit der IHK zu Kiel wird darin unter der Überschrift „Bahn frei für Web 2.0 in Schleswig-Holstein“ geworben u. a. mit folgenden Zitaten: „Damit widerlegen wir die Auffassung des Unabhängigen Landeszentrums für Datenschutz, wonach der Betrieb so genannter Fanpages gegen deutsches Datenschutzrecht verstößt“ und „Ein wichtiges Signal für Unternehmen in Schleswig-Holstein: Es geht eben doch“[5].

Ich habe das Lorenz-von-Stein-Institut bisher immer als eine juristisch seriös argumentierende Einrichtung angesehen. Dass der Klappentext für das neue Buch allzu sehr im Interesse des Kooperationspartners IHK ausfällt, muss wohl als medialer Ausrutscher hingenommen werden. Der Blick ins Buch selbst offenbart, dass die Autoren dem ULD – in vieler Hinsicht vielleicht unfreiwillig – Recht geben und nur mit einigen rechtlichen Verrenkungen zum gewünschten Ergebnis kommen.



Die Hauptargumentation von Facebook ist, dass die Mitglieder mit ihrer Teilnahme der Datenverarbeitung des Unternehmens in den USA zugestimmt hätten. Die Autoren meinen nun, dass diese Einwilligung den „deutschen Datenschutzvorschriften nicht gänzlich genügen mag“ (S. 189), so als gäbe es im Recht die Kategorie „nur ein bisschen unzulässig“. Dass bei dem Facebook-Angebot gegen Telemedienrecht verstoßen wird, wird zwar nicht ausführlich geprüft, aber stillschweigend konzediert (S. 180 f.).

IV. Krude Verantwortungsethik

Der Versuch, die Verantwortung für die illegale Datenverarbeitung von Facebook abzustreifen, erfolgt über mehrere Schritte. Zunächst wird korrekt bestätigt, dass der Fanpage-Betreiber telemedienrechtlich für sein Tun verantwortlich ist. Dies könne auf den Datenschutz nicht voll übertragen werden, denn: Er kann „lediglich entscheiden, einen Facebook-Account zu eröffnen, um hierüber eine Fanseite zu erstellen, oder dies zu unterlassen. Weitergehende Entscheidungsmöglichkeiten hat er nicht“ (S. 182). Entsprechend könnte man auch argumentieren: Mache ich mich also zum Komplize eines bösen Buben und kann ich den bösen Buben von seinem bösen Tun nicht abbringen, dann kann ich Komplize bleiben und meine Hände in Unschuld waschen.

Es kommt noch besser nach dem Motto: Wir haben von all dem nichts gewusst: „Des Weiteren wird dem Fanseiten-Betreiber das Ausmaß und der Umfang der Datenerhebung und -verarbeitung nur unzureichend bekannt sein“ (S. 182). „Der Fanseiten-Betreiber weiß grundsätzlich nur so viel über die Datenerhebung, wie Facebook ihm offenbart“ (S. 184). Zwar dürften die ausführlichen Geschäftsbedingungen von Facebook den Betreibern zugänglich sein; auch die umfassenden Analysen der Datenschutzbehörden und des ULD dürften zumindest den Behörden und größeren kommerziellen Anbietern in Schleswig-Holstein bekannt sein. Statt nun die Finger vom Unbekannten zu lassen, erklärt man sich bei dessen Nutzung einfach für unverantwortlich. Dies ist nicht nur rechtlich falsch, sondern Ausdruck einer in letzter Konsequenz grausamen Verantwortungsethik.

Es wird noch besser: Schuld sind eigentlich die Nutzer: „Letztlich haben sich alle Nutzer freiwillig angemeldet und tolerieren daher die Datenerhebung von Facebook. … Dieser Einwilligung … muss zumindest eine gewisse Teillegitimation, wenn auch nicht zwingend gegenüber Facebook, dann jedoch gegenüber den ebenfalls bei Facebook präsenten öffentlichen und nichtöffentlichen Stellen zukommen“ (S. 189). Also: Die schlecht informierten Betreiber sind nicht verantwortlich, wohl aber – die in der Regel noch schlechter informierten – Nutzer. Ob das so richtig sein kann?

V. Verhältnismäßigkeit statt Gesetzesvorbehalt

Die Autoren bestreiten nicht, „dass personenbezogene Daten durch Facebook (am Maßstab deutschen Datenschutzrechts gemessen in unzulässiger Weise) erhoben und verarbeitet werden“ (S. 187). Geleugnet wird auch

nicht die „Rechtsbindung der deutschen Verwaltung aus Art. 20 Abs. 3 GG und der Schutzverpflichtung gegenüber den Persönlichkeitsrechten der Nutzer“ (S. 187). Doch dann behaupten sie, „mangels gesetzlicher Regelungen“ (S. 187) müsse eine „Abwägung von Risiko und Nutzen“ (S. 188) erfolgen. Es gäbe auf dieser Ebene „keine ‚Schwarz-Weiß-Sicht bzw. -Lösung‘ (im Sinne des ULD und eine (vermeintlich) klare Rechtslage“ (S. 187). Dies verwundert, haben wir doch in Deutschland und Europa ein umfassendes Datenschutzrecht. Doch gibt es eine Erklärung: „Das deutsche Datenschutzrecht ist … nicht auf derartige neue Technologien ausgerichtet und wird so der Funktionsweise des Internet nicht mehr gerecht“ (S. 189). Auch wenn das zutrifft, so sollte man sich die bestehenden geltenden Regelungen doch genauer anschauen und nicht gleich das ganze Recht über Bord werfen.

Hat sich die Argumentation derart von einer Gesetzesbindung gelöst, muss nur noch abgewogen werden: „Der immense Nutzen, den eine Facebook-Fanseite hat, darf jedoch nicht außer Betracht gelassen werden. Facebook ist das weltgrößte Internetnetzwerk und bietet deshalb eine sehr große ‚Community‘ … Durch eine Facebook-Präsenz können daher (mit geringem Aufwand) mehr Menschen erreicht werden als mit einer herkömmlichen Internetpräsenz“ (S. 188). „Gerade jüngere Generationen (‚Digital Natives‘) nutzen Facebook nahezu flächendeckend und regelmäßig, sodass diese Gruppe über Facebook besonders angesprochen werden kann“ (S. 189). Erstaunlich ist, dass von den Autoren die Datenschutzverstöße von Facebook nicht explizit benannt, geschweige denn analysiert werden, so dass auch die Risiken für die Betroffenen nicht seriös abgewogen werden können. Vielmehr wird die Relevanz der Facebook-Präsenz heruntergespielt: „Hinzuweisen ist zudem darauf, dass es sich bei der Öffentlichkeits- und Informationstätigkeit überwiegend um eine ‚freiwillige‘ Aufgabe der öffentlichen Verwaltung handelt – mit der Folge, dass die Verlagerung auf andere Medien weitaus unkritischer sein dürfte als z. B. ausschließlich elektronisch durchführbare Verwaltungsverfahren“ (S. 190).

VI. Wie geht es weiter?

Eine Alternative zur Nutzung von Facebook, Google+ & Co. wird von den Autoren benannt: „So wäre der Staat gezwungen, eigene ‚nationale‘ Tools aufzubauen oder zu subventionieren“ (S. 185). Aber das ist nicht deren Ziel. Wohl muss Folgendes gelten: Bei allen informationstechnischen Systemen, die staatliche Stellen einsetzen, müssen diese kontrollieren und nachvollziehen können, dass das Datenschutzrecht eingehalten wird.

Die Autoren erweisen ihren Auftraggebern einen Bärendienst und tun dem Datenschutz unfreiwillig einen Gefallen, indem sie ihre eigenen rechtlichen Argumente ad absurdum führen, so dass sich die Richtigkeit der Argumente der Datenschutzbehörden aufdrängt. Jedenfalls kann von einem „Widerlegen“ der Auffassung des ULD keine Rede sein.

Zu hoffen ist nun auf das von den Staatskanzleien der Länder in Auftrag gegebene und schon für den Dezember 2011 angekündigte Gutachten der Innenministerkonferenz. Nach Mitteilung des Landesinnenministeriums im Innen- und Rechtsausschuss des Schleswig-Holsteinischen Landtags am 15.02.2012 liegt ein Entwurf dieses Gutachtens vor und wird hoffentlich – nach einer Abstimmung zwischen den Ländern – zeitnah veröffentlicht. Zu hoffen ist weiterhin, dass dieses Gutachten zum gleichen Ergebnis kommt wie sämtliche Datenschutzbeauftragten des Bundes und der Länder, die die Position des ULD bestätigten[6]. Sollte dies nicht der Fall sein, so besteht noch die Hoffnung auf die Verwaltungsgerichtsbarkeit. Inzwischen liegen zwei Anfechtungsklagen gegen Untersagungsverfügungen des ULD vor, eine davon der Wirtschaftsakademie der IHK; leider liegen dem ULD bis heute keine Klagebegründungen vor. Da der mehrstufige Instanzenzug im Verwaltungsrechtsweg lange dauern kann, ist eine endgültige verbindliche Entscheidung aber auch hier nicht schnell zu erwarten.

Also: Die Verzweiflung hält weiter an. Doch: Die Diskussion geht in die nächsten Runden. Die europäischen Datenschutzbehörden befassen sich intensiv mit den Themen. Und die Europäische Kommission hat mit ihrem Vorschlag für eine „Datenschutz-Grundordnung“ vom 25.01.2012 den Grundstein für ein einheitliches Datenschutzrecht in Europa gelegt, das den technischen Gegebenheiten des Internet und von Sozialen Netzwerken besser gerecht wird[7]. Wäre diese Grundverordnung schon in Kraft, so gäbe es wirksame Instrumente zum Datenschutz bei Sozialen Netzwerken; die Rechtswidrigkeit der Angebote von Facebook, Google+ & Co. könnte auch durch Stellen in Schleswig-Holstein nicht mehr bestritten werden.

1 Es muss ausdrücklich darauf hingewiesen werden, dass die Landesverbände sowohl von Bündnis 90/Die Grünen als auch der Piratenpartei aus Datenschutzgründen keine Facebook-Fanpage betreiben, vgl. Wacker, http://landesblog.de/2012/01/grune-werden-mit-facebook-nicht-grun-facebook-fanpage-soll-geloscht-werden/.

2 Presseerklärung des ULD vom 09.12.2011, https://www.datenschutzzentrum.de/presse/20111209-facebook-duesseldorfer-kreis.htm.

3 Gemeinsame Pressemitteilung CDU- und FDP-Landtagsfraktion vom 06.12.2012, http://www.ltsh.de/presseticker/2011-12/06/16-04-59-792b/.

4 Hrsg. Utz Schliesky/Sönke Schulz, ISBN 978-3-936-773-71-2, 39,00 Euro.

5 Presseinformation 47/2012 der CAU vom 20.02.2012, http://www.uni-kiel.de/aktuell/pm/2012/2012-047-web20-buch.shtml.

6 Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) vom 08. Dezember 2011, https://www.datenschutzzentrum.de/internet/20111208-DK-B-Soziale-Netzwerke.html.

7 Europäische Kommission vom 25.01.2012, KOM(2012)9 endgültig, Der Schutz der Privatsphäre in einer vernetzten Welt – Ein europäischer Datenschutzrahmen für das 21. Jahrhundert.

Datenschutznachrichten

Datenschutznachrichten aus Deutschland

Bund

Hunderttausendfache Nutzung von „stiller SMS“

Polizei, Zoll und Verfassungsschutz lokalisieren Verdächtige per „stiller SMS“. Die technischen Möglichkeiten von Handys und Smartphones bieten nicht nur den Nutzenden Vorteile, sondern erlauben es Sicherheitsbehörden, die Besitzenden zu orten, ohne dass diese etwas davon bemerken. Mit „stillen SMS“ können diese herausfinden, in welcher Funkzelle bzw. zwischen welchen Funkzellen sich ein Mobiltelefon gerade befindet. Bei der „stillen SMS“ wird ein Signal an das Handy der Zielperson gesendet, das dort keine für den Benutzenden sicht- oder hörbare Reaktion auslöst. Das Handy nimmt dabei mit der nächsten Funkzelle Kontakt auf, so dass der Netzbetreiber den ungefähren Standort erfährt, die sich die Sicherheitsbehörde dann vom Provider mitteilen lässt. Es handelt sich also um eine Kurznachricht ohne Inhalt und mit einem Steuerbefehl, der dafür sorgt, dass auf dem Handy weder etwas angezeigt wird noch für den Betroffenen ein erkennbares Signal ausgegeben wird. Nur wenn das Handy z. B. neben einem eingeschalteten Lautsprecher liegt, könnte der Überwachte durch ein erkennbares Störgeräusch Verdacht schöpfen. Die Daten, die das Handy zurückmeldet, laufen bei den Betreibern der Mobilfunknetze auf und werden in den meisten Fällen über eine gesicherte Datenleitung direkt an die Ermittler weitergeleitet. Manchmal erfolgt die Datenweitergabe auf einem Datenträger oder per Fax. Der Radius einer Funkzelle beträgt je nach Technik, Landschaft und Bevölkerungsdichte etwa hundert Meter bis einige Kilometer. Die Polizei nutzt „stille SMS“ regelmäßig, um Verdächtige, deren Handynummer sie kennt, aufzufinden und festzunehmen. Beim Verfassungsschutz werden mit diesem Trick Bewegungsbilder einer Person erstellt oder Observationen unterstützt.

Der Bundestagsabgeordnete Andrej Hunko von der Fraktion Linke wollte von der Bundesregierung genau wissen, wie oft ihre Sicherheitsbehörden „stille SMS“ an Verdächtige senden. Gemäß der Antwort verschickte im Jahr 2010 das Bundeskriminalamt (BKA) 96.314 „stille SMS“, das Bundesamt für Verfassungsschutz (BfV) 107.852 und die Zollfahndungsbehörden sogar 236.617. Bundespolizei und Militärischer Abschirmdienst haben angeblich keine Statistik. Von 2006 bis 2011 waren es beim BKA mehr als 355.000 SMS, beim BfV knapp 400.000 und beim Zoll mehr als 950.000. Eine besondere Zunahme erfolgte im Jahr 2011 beim Zoll: Dessen Fahndungsbehörden haben in der ersten Hälfte 2011 mit 227.587 Ortungsnachrichten bereits fast so viele stille SMS versandt wie im gesamten Vorjahr. Dazu kommen noch die Zahlen aus den Ländern. Bekannt sind diese aus Nordrhein-Westfalen, wo sie die Linken-Abgeordnete Anna Conrads jüngst abgefragt hat. Im Jahr 2010 hat die Polizei dort 255.874 „Ortungsimpulse“ (so der Polizei-Jargon für „stille SMS“) abgesandt. Die Zahl der betroffenen Handys liegt aber deutlich niedriger. In NRW waren in 778 Ermittlungsverfahren 2.644 Mobiltelefone betroffen. Das heißt, pro Mobiltelefon verschickte die Polizei im Schnitt rund 100 „stille SMS“ (s. u. S. 25). Beim BfV waren pro Jahr 90-150 Mobiltelefone betroffen, wie ein Sprecher auf eine Presseanfrage mitteilte. Wenige Handys wurden also besonders intensiv überwacht.

Bekannt wurde der Einsatz von „stillen SMS“ durch die Polizei erstmals 2003 in Berlin (DANA 2/2003, 15; 3/2003, 15 f.; 4/2003, 11 f). In der Folge gab es einige wissenschaftliche Aufsätze, die die Ermittlungsmethode mangels Rechtsgrundlage für unzulässig erklärten. Entsprechende Gerichtsurteile sind nicht bekannt. Seit 2008 gibt es eine gesetzliche Regelung. Die große Koalition regelte in der so genannten „TKÜ-Novelle“ die heimlichen Ermittlungsmaßnahmen in der Strafprozessordnung neu. Dabei wurde der Polizei unter anderem erlaubt, dass sie beim Mobilfunkprovider nicht nur „Verbindungsdaten“, sondern auch „Verkehrsdaten“ verlangen darf. Sie muss nun nicht darauf warten, bis der Verdächtige telefoniert oder mittels „stiller SMS“ in eine Verbindung getrickst wird, sondern sie kann schon die Daten der regelmäßigen Kontaktaufnahme des Handys mit dem Netzbetreiber abfragen. In der Begründung zur Neufassung von Paragraph 100g hieß es: „Die Neuregelung kann die - rechtlich umstrittene - Übersendung einer ‚stillen SMS‘ entbehrlich machen“. Dieser Paragraph wird auch für die Funkzellenabfrage herangezogen, die im Februar 2011 in Dresden massenhaft genutzt wurde (DANA 3/2011, 119 ff.). Nach Ansicht von Constanze Kurz vom Chaos Computer Club ist die Rechtslage unklar: „Ein Handy ist eine Ortungswanze, das müsste gesetzlich beschränkt werden. Es ist ausgeufert“.

Die aktuellen Zahlen zeigen, dass die „stille SMS“ aus Sicht der Polizei unentbehrlich geworden ist. Sie bringt genauere Daten als die Kommunikation von Basisstation und Handy. Dort wird die Location Area des Handys bekannt, also der Zusammenschluss mehrerer Funkzellen; die Kontaktaufnahme erfolgt in der Regel nur einmal am Tag. Dagegen verrät ein Kontakt per „stiller SMS“ die konkrete Funkzelle. Und je nach Ermittlungsziel können die Behörden sogar alle paar Minuten einen neuen Ortungsimpuls senden. Als eigenständige Maßnahme geregelt ist die „stille SMS“ heute immer noch nicht. Das Problem dürfte nach der Neuregelung zwar nicht mehr die Herausgabe der Standortdaten sein. Fraglich bleibt, ob die Polizei einem Verdächtigen ohne

Rechtsgrundlage „stille SMS" schicken darf. Polizeinahe JuristInnen verweisen darauf, dass die Ermittler einen Verdächtigen ja auch zum Schein anrufen dürfen, um seine Anwesenheit zu Hause zu kontrollieren. Der Vergleich hinkt jedoch insofern, dass ein solcher Anruf für den Betroffenen hörbar ist, während die „stille SMS" heimlich erfolgt und deshalb beliebig oft wiederholt werden kann, so dass eine ganz andere Überwachungsdichte möglich ist.

Derzeit finden wohl alle polizeilichen SMS-Ortungen im Rahmen einer richterlich genehmigten Handy-Überwachung statt. Wenn bei Gefahr im Verzug zunächst die Staatsanwaltschaft entscheidet, muss das Gericht spätestens nach drei Tagen zustimmen. Der Einsatz durch den Verfassungsschutz erfolgt nur, wenn eine Handy-Überwachung im so genannten G-10-Kontrollgremium des Parlaments genehmigt wurde. Die Betroffenen werden gemäß der gesetzlichen Regelung - nachträglich - zumeist über die Handy-Überwachung unterrichtet. Der Einsatz von „stillen SMS" wird dabei aber, so das BKA, nicht thematisiert. Dies ist wohl eine Erklärung dafür, warum es keine Klagen zur Zulässigkeit der Methode gibt. Die Betroffenen wissen einfach nichts davon. Aus Sicht des Justiz- und des Innenministeriums des Bundes besteht hinsichtlich der Verwendung dieser Methode kein politischer Handlungsbedarf. Eine Sprecherin des Bundesjustizministeriums meinte: „Darüber müssen die Gerichte entscheiden." Wer sicher gehen will, dass er nicht per „stiller SMS" geortet werden kann, muss nicht nur das Handy ausschalten, sondern auch die SIM-Karte oder den Akku entfernen (Krempl www.heise.de 13.12.2011; Rath www.taz.de 02.01.2012; Thieme www.fr-online.de 03.01.2012; SZ 03.01.2012, 5; Martin-Jung SZ 05./06.01.2012, 20; vgl. die umfassende Anfrage BT-Drs. 17/8257).

Bund

Visa-Warndatei wird aufgebaut

Das am 01.12.2011 vom Bundestag verabschiedete „Gesetz zur Errichtung einer Visa-Warndatei und zur Änderung des Aufenthaltsgesetzes" wurde am 29.12.2011 im Bundesgesetzblatt verkündet. Es tritt am 01.06.2013 in Kraft. Nun beginnt die technische Umsetzung der Datei, die in erster Linie der Unterstützung der Visumbehörden im Visumverfahren und damit der Bekämpfung der illegalen Einreise dienen soll. In der Datei gespeichert werden Visumantragstellende, Einladende, Verpflichtungsgebende und sonstige Referenzpersonen, die mit Verurteilungen wegen bestimmter Straftaten mit Bezug zum Visumverfahren oder mit sonstigem Auslandsbezug oder mit ganz speziellen sonstigen rechtswidrigen Verhaltensweisen wie insbesondere falschen Angaben im Visumverfahren aufgefallen sind. Darüber hinaus soll mit der Schaffung eines weiteren Datenabgleichsverfahrens sicherheitspolitischen Interessen im Visumverfahren Rechnung getragen werden. Dazu wird beim Bundesverwaltungsamt (BVA) eine besondere Organisationseinheit errichtet, bei der Daten aus dem Visumverfahren mit bestimmten Daten aus der Antiterrordatei automatisiert abgeglichen werden. Durch den automatisierten Abgleich soll eine Rückmeldung durch Sicherheitsbehörden an die Visumbehörden ermöglicht werden, wenn Personen aus dem terroristischen Umfeld beabsichtigen, nach Deutschland einzureisen (BGBl. I, S. 3037; Kurzmeldung Bundesministerium des Innern 12.01.2012; www.bmi.bund.de; vgl. DANA 4/2010, 149).

Bund

Elektronischer Aufenthaltstitel eingeführt

Mit Datum vom 01.09.2011 wurde in Deutschland der elektronische Aufenthaltstitel (eAufenthaltstitel) als eigenständiges Dokument im Scheckkartenformat für Drittstaatenangehörige, also für Staatsangehörige von Nicht-EU-Staaten, eingeführt. Er ersetzt damit den bisherigen Aufenthaltstitel als Klebeetikett im Pass bzw. Reisedokument. Damit werden die europäischen Vorgaben zur einheitlichen Gestaltung des Aufenthaltstitels für Drittstaatenangehörige umgesetzt. Die einschlägigen EU-Verordnungen (EG Nr. 1030/2002 und 380/2008) verpflichten alle Mitgliedstaaten der Europäischen Union (EU), einen einheitlichen Aufenthaltstitel mit biometrischen Merkmalen auszustellen.

Der eAufenthaltstitel besitzt einen Chip im Karteninneren, auf dem die persönlichen Daten, ggfs. aufenthalts- bzw. erwerbstätigkeitsrechtliche Auflagen sowie die biometrischen Merkmale, also Lichtbild und zwei Fingerabdrücke, gespeichert sind. Die biometrischen Daten dürfen ausschließlich von hoheitlichen Stellen wie z. B. Ausländerbehörden oder der Polizei ausgelesen werden. Sie sollen vor Fälschungen und Missbrauch schützen und damit einen Beitrag zur Verhinderung und Bekämpfung der illegalen Einwanderung und des illegalen Aufenthalts leisten. Die Karte ist technisch mit dem neuen Personalausweis für deutsche Staatsangehörige vergleichbar. Der eAufenthaltstitel besitzt die gleichen elektronischen Zusatzfunktionen: So können die InhaberInnen die Online-Ausweisfunktion in Anspruch nehmen, z. B. für Online-Shops oder Behörden-Anwendungen, soweit diese hierfür eingerichtet sind. Anmeldungen in Internetportalen und der Altersnachweis im Internet sind darüber möglich. Den Zugriff auf die Daten erhalten ausschließlich Anbieter, die ein staatliches Berechtigungszertifikat besitzen.

Darüber hinaus ist der eAufenthaltstitel für die Qualifizierte Elektronische Signatur (QES) vorbereitet. Mit der Signatur können rechtsgültig digitale Dokumente, z. B. Verträge, unterzeichnet werden. Ein dafür notwendiges Zertifikat können die InhaberInnen bei einem Signatur-Anbieter am Markt erwerben. Für Drittstaatenangehörige, die derzeit einen gültigen Aufenthaltstitel als Klebeetikett besitzen, änderte sich zum 01.09.2011 zunächst nichts. Die bisher ausgestellten Aufenthaltstitel behalten ihre Gültigkeit. Erst bei einer späteren Verlängerung oder Neuausstellung wird der Aufenthaltstitel als eAufenthaltstitel ausgestellt. Die Aufenthaltstitel werden weiterhin in der Ausländerbehörde beantragt. Neu zu berücksichtigen ist die Produktionszeit und die dadurch bedingten längeren Ausstellungszeiten in den Ausländerbehörden. Zur Antragstellung ist das persönliche Erscheinen in der

Ausländerbehörde 4 bis 6 Wochen vor Ablauf der Gültigkeit des bisherigen Aufenthaltstitels erforderlich (www.bmi.bund.de, PM BMI 23.08.2011).

Baden-Württemberg

Staatstrojanereinsatz im Fall Bögerl

Der umstrittene Staatstrojaner ist offenbar bei den Ermittlungen im Fall der ermordeten Heidenheimer Bankiers-Ehefrau Maria Bögerl eingesetzt worden. Im Familien- und Freundeskreis der Bögerls wurden demgemäß auch Telefone überwacht. Auch eine Therapeutin, die die Angehörigen psychologisch betreut hatte, sei betroffen. Diese sei von der Einstellung der Abhörmaßnahme von der Staatsanwaltschaft informiert worden. Bögerl war am 12.05.2010 aus ihrem Haus verschwunden und drei Wochen später erstochen aufgefunden worden. Es gibt bis heute keinen Hinweis auf den Täter. Ihr Ehemann, der Heidenheimer Sparkassen-Vorstand Thomas Bögerl, nahm sich im Juli 2011 das Leben. Nachdem der Chaos Computer Club (CCC) im Oktober 2011 Details über den Staatstrojaner veröffentlicht hatte, die auf massive Rechtsverstöße hinwiesen, stoppte der Innenminister von Baden-Württemberg Reinhold Gall (SPD) den Einsatz der Spionagesoftware. Seinen Angaben zufolge wurde die Maßnahme vier Mal eingesetzt (Der Spiegel 3/2012, 14; www.taz.de 15.01.2012).

Berlin

Funkzellenabfrage zur Aufklärung von Brandstiftungen

Die Berliner Polizei hat im Fall des mutmaßlichen Serienbrandstifters André H. Funkzellenabfragen durchgeführt. Ein Sprecher der Staatsanwaltschaft bestätigte, dass die umstrittene Maßnahme bei den Ermittlungen „in mehreren Fällen" eingesetzt wurde. Die Ermittler stellten fest, dass das Handy des Verdächtigen zur Tatzeit in der Nähe des Tatorts aktiv gewesen sei. Der Mann war im Oktober 2011 festgenommen worden und hatte 67 Brandstiftungen eingeräumt. Mittlerweile gehen die Ermittler sogar davon aus, dass er in über 100 Fällen Autos angezündet und weitere beschädigt hat. Bei der Verhaftung des Verdächtigen hatten die Behörden bei der Darstellung der Fahndung dieses wichtige Detail verschwiegen. Damals stellte die Polizei den Fall so dar: Man sei dem Mann durch die Auswertung von Überwachungsvideos aus Haltestellen auf die Spur gekommen. Der später Verhaftete sei Fahndern aufgefallen, weil er kurz vor und nach Brandanschlägen auf Überwachungsfilmen zu sehen war. Polizisten hätten André H. „später zufällig identifizieren" können, hieß es damals.

Auf Antrag der Piraten diskutierte das Berliner Abgeordnetenhaus die Überprüfung von Handydaten bei der Suche nach Autobrandstiftern. Dabei ergab sich, dass die Polizei in über 800 weiteren Fällen Handydaten überprüfte. Komplett konträre Sichtweisen prägten die Auseinandersetzung um die Handy-Überwachung, bei der seit 2008 rund 4,2 Millionen Datensätze ausgewertet und 960 Handyeigentümer namentlich identifiziert wurden. Sahen SPD- und CDU-Fraktion sowie Innensenator Frank Henkel (CDU) bei der Überwachung alles im legalen Bereich, so war das bei Grünen, Linkspartei und Piraten ganz anders. „Nicht alles, was der Staat kann, soll er auch dürfen", sagte Grünen-Innenpolitiker Benedikt Lux. Jeder Eingriff in die Unschuldsvermutung sei zu vermeiden. Lux rückte die Vorgänge in die Nähe der noch umfangreicheren Datenüberprüfung im vergangenen Jahr bei einer Anti-Nazi-Demonstration in Dresden (DANA 3/2011, 119). „Was dort passiert ist, war ein Skandal, und das darf sich hier in Berlin nicht wiederholen." Den Piraten-Vorstoß, alle Betroffenen über SMS über die Erfassung zu informieren, nannte er „völligen Unsinn": Dies sei ein weiterer Eingriff, weil man die Daten verwerte. Die Piraten bestritten das. Linkspartei-Rechtsexperte Klaus Lederer sprach von einem „handfesten Überwachungsskandal" und forderte, das Instrument der Handydaten-Abfrage ersatzlos zu streichen. Wie Lux und Christopher Lauer (Piraten) konnte er mangels Fahndungserfolg keinen Sinn und nur Rechtsverletzungen darin erkennen. Lauer kritisierte: „Unverdächtige kommen durch diese Maßnahmen in Verdacht."

Nach Ansicht der CDU will die Linkspartei lediglich von eigenen Fehlern ablenken. Innensenator Henkel mochte nicht akzeptieren, dass sie nach Worten ihres Fraktionschefs Udo Wolf nichts von der Überwachung wusste, die 2008 unter rot-roter Regierung begann. Einen von Wolf ins Gespräch gebrachten Untersuchungsausschuss hält er für überflüssig. „Ich weiß nicht, was Sie dort untersuchen wollen: Die rechtlichen Grundlagen können Sie sich in jeder Bibliothek rauslesen." Die Polizei habe sich an Recht und Gesetz gehalten. Sein Fraktionskollegen Robbin Juhnke kritisierte die Opposition: „Sie tun ja gerade so, als ob die Polizei mit Hilfe einer perfiden Apparatur die Träume von halb Friedrichshain aufgezeichnet hätte." In Richtung des Grünen Lux sagte Henkel, die Fälle in Dresden seien „mit denen in Berlin nicht vergleichbar". Nach Angaben von Staatssekretär Bernd Krömer (CDU) hat die Polizei über die debattierte Datenabfrage hinaus bei den mehr als 800 Fällen auch bei nicht politisch motivierten Straftaten Handydaten überprüft. SPD-Innenpolitiker Thomas Kleineidam mochte nicht bestreiten, dass die Datenabfrage in Grundrechte eingreife, wichtig sei hier eine Abwägung. Videoaufzeichnungen - sie und nicht die Datenabfragen hätten zur Überführung des Brandstifters geführt - stellen für ihn einen viel größeren Eingriff dar. Kleineidam lehnt es wie Henkel ab, auf die Datenabfrage zu verzichten: „Ich kann mir vorstellen, das auch in Zukunft einzusetzen. Grundsätzlich geeignet ist es sehr wohl, auch wenn es hier keinen Erfolg hatte." Berlins Datenschutzbeauftragter Alexander Dix meinte: „Es ist unbestritten, dass es sich bei Autobrandstiftungen um schwere Straftaten handelt." Angesichts der unklaren Rechtslage sei es „dringend geboten", mit Sachsen für eine Gesetzesänderung einzutreten (www.spiegel.de 22.01.2012; von Bullion SZ 24.01.2012, 1, 5; Alberti www.taz.de 26.01.2012).

Berlin

Soziale Bewegungen im digitalen Tsunami – Tagung in Berlin am 4. Februar 2012

ExpertInnen aus der Datenschutzpraxis und AktivistInnen aus den sozialen Bewegungen brachte am 4. Februar 2012 eine Tagung in Berlin-Kreuzberg zusammen, um gemeinsam Reaktionen auf die Überwachungsanfälligkeit moderner Kommunikationsmittel, die Wirksamkeit verschiedener Gegenstrategien und Fragen des digitalen Selbstschutzes zu erörtern.

Unter dem Titel „Soziale Bewegungen im digitalen Tsunami" diskutierten unter anderem Rechtsanwalt Peer Stolle (RAV), Erich Moechel, Eric Töpfer (Statewatch/ CILIP), Ralf Bendrath, Renat Tangens (foebud) und Thilo Weichert (ULD) die Entwicklung und Anwendung von moderner Überwachungstechnologie mit VertreterInnen aus sozialen Bewegungen und NetzaktivistInnen. Die Beiträge auf den drei Podien, an denen u.a. auch Matthias Monroy (Gipfelsoli), Katharina Nocun (AK Vorrat), Sandra Mamitzsch (Digitale Gesellschaft e.V.) und ein Vertreter von nadir.org teilnahmen, sind im download zu hören auf http://netzpolitik.org/2012/livestream-soziale-bewegungen-im-digitalen-tsunami/. S. auch taz v. http://www.taz.de/!86966/.

Berlin

Polizei beschafft sich Staatstrojaner von Syborg

Die Polizei in Berlin beschafft sich nach Angaben von Innensenator Frank Henkel zur Ausspähung von Computern von Verdächtigen für 280.000 Euro einen Trojaner der Firma Syborg. Die Piratenpartei hatte eine große Anfrage gestartet. Aus der Antwort ergibt sich, dass der Auftrag für den Berlintrojaner erteilt ist. Christopher Lauer von der Piratenpartei: „Die Software darf nicht zum Einsatz kommen. Wenn Herr Henkel wider besseren Wissens diese Software nutzen lässt, dann ist der nächste Skandal vorprogrammiert." Lauer und sein Kollege Alexander Morlang meinen, dass eine rechtlich saubere Nutzung eines Trojaners nicht machbar sei. „Das Bundesverfassungsgericht hat Schranken für den Einsatz von Quellen-Telekommunikationsüberwachung und Online-Durchsuchung gesetzt, die sich technisch nicht umsetzen lassen." Henkel hatte hingegen betont, der Einsatz einer solchen Software könne rechtmäßig erfolgen und sei für die Ermittlungsarbeit notwendig. Nicht nur die Piratenpartei kritisierte den Einsatz eines Trojaners. Auch Klaus Lederer, Sprecher der Linkspartei für Recht und Verbraucherschutz im Abgeordnetenhaus, nannte den Berlintrojaner unvereinbar mit der Verfassung.

Die saarländische Firma Syborg hatte im Oktober 2011 zur Staatstrojaner-Affäre mitgeteilt, man gebe „generell keine Auskunft über Kunden, potentielle Kunden oder Lösungen". Im Dezember äußerte sich der Firmenchef dann doch: Bei eine Recherche waren Journalisten in Libyen auf Unterlagen der Firma gestoßen. Dabei handelte es sich offenbar um ein Angebot. Syborg-Chef Robert Lander erklärte darauf, sein Unternehmen habe „bis dato keinerlei Geschäfte mit beziehungsweise in Libyen getätigt" (Reißmann www.spiegel.de 27.01.2012).

Hessen

Heimliche Videoüberwachung bei Maredo führt zu Kündigungen

Die Steakhaus-Kette Maredo soll die überwiegend ausländischen MitarbeiterInnen unter Druck gesetzt haben, indem sie diese per Video überwachte und dazu aufforderte, ihre Handys während der Arbeitszeit abzugeben, damit sie nicht mehr telefonieren können. Gerhard Jahn, 59jähriger Sekretär bei der Gewerkschaft Nahrung, Genuss, Gaststätten (NGG), meinte, er habe in seinen zwei Jahrzehnten Tätigkeit „einen solchen Fall noch nicht erlebt: Das ist einmalig in Deutschland." Bezug genommen wird damit auf den 26.11.2011, als im Restaurant der Steakhaus-Kette Maredo in der Frankfurter Fressgasse 34 Beschäftigte, mehrheitlich MigrantInnen, von Sicherheitsmitarbeitern in der Filiale festgehalten und „zu Eigenkündigungen gezwungen wurden". Bei der Staatsanwaltschaft Frankfurt haben 14 Angestellte danach Strafanzeige wegen Freiheitsberaubung und Nötigung gestellt. Ein Sprecher der Maredo-Zentrale in Düsseldorf bestritt strikt die Vorwürfe: „Es ist niemand festgehalten worden, jeder konnte gehen oder telefonieren." Maredo erklärte, die MitarbeiterInnen in der Filiale Große Bockenheimer Straße 24 durch Videokameras und verdeckte Ermittler zuvor überwacht zu haben. Es sei regelmäßig zu Diebstählen von Lebensmitteln und anderem Firmenbesitz gekommen. „In einer Woche wurden allein 500 Vergehen dokumentiert." Im Februar 2011 begann die Überwachungsaktion mit dem Hinweis eines Mitarbeiters gegenüber dem Filialleiter: „Die Leute klauen wie die Raben." Nun meint die Firma, mit den Aufnahmen der Videokameras belegen zu können, dass 29 Beschäftigte an den Diebstählen beteiligt gewesen seien. Über die Höhe des entstandenen Schadens ließen sich keine Angaben machen. Ein Unternehmenssprecher meinte: „Wir wundern uns, dass die Gewerkschaft Leute schützt, die klauen".

Die Videokameras wurden laut Gewerkschaftssekretär Jahn „illegal, ohne Wissen der Beschäftigten installiert – und zwar so, dass sie nicht zu sehen waren". Zwei verdeckte Ermittler hätten zudem im Auftrag von Maredo in der Zweigstelle gearbeitet – „der eine 14 Tage, der andere vier Wochen". Am 26.11.2011 fiel etwa um 13 Uhr der Strom aus. Nach Darstellung der Gewerkschaft habe Maredo so dafür gesorgt, dass die Gäste das Haus verließen und man unter sich war. „Die rückten mit einem großen Stab aus der Zentrale in Düsseldorf an, darunter der Hauptpersonalchef und Sicherheitsleute." Der Sprecher des Unternehmens meinte dagegen, es habe sich um einen normalen „Stromausfall" gehandelt, der später „repariert" wor-

den sei. Niemand sei gezwungen worden, die Firma zu verlassen: „Wir wollten angesichts der Diebstähle den Leuten die Gelegenheit geben, selbst zu kündigen." Tatsächlich habe Maredo 16 Kündigungen ausgesprochen, 13 MitarbeiterInnen hätten „von selbst gekündigt". Zwei dieser freiwilligen Kündigungen seien später wieder zurückgenommen worden. Einige der Betroffenen wehren sich nun vor dem Arbeitsgericht Frankfurt gegen ihre Kündigung (Göpfert, www.fr-online.de 18.01.2012).

Hessen

Elterliche Kontrolle führte zu gegenseitigen Hacking-Angriffen

Ein junger Hacker ärgerte einen misstrauischen Vater – und löst damit eine Debatte über die Sicherheitsvorkehrungen bei der Polizei aus. Der Vater ist Beamter im gehobenen Dienst bei der Bundespolizei, und von seinem privaten Rechner kamen interne Dokumente abhanden. Der Vater wollte herausfinden, was seine Tochter im Internet treibt, und spielte ihr einen Trojaner auf den Rechner. Das fand ein Freund des Mädchens heraus. Der junge Mann, in der Hacker-Szene tätig, zahlte es dem neugierigen Papa heim, schaut sich auf dessen Computer um und lud Dokumente herunter. Die Dokumente, die er auf seinem Rechner gespeichert hatte, waren dienstlicher Art. Es handelte sich um Kommunikationspläne: Wer muss wen in welchem Fall unter welcher Nummer anrufen. Viel anfangen konnte der junge Mann damit nicht, die Dokumente waren nur für den internen Gebrauch nützlich; zudem sollen sie nicht auf dem aktuellen Stand gewesen sein. Dass der Polizist sie nicht auf dem Rechner hätte speichern dürfen, ist jedoch unstrittig.

Die Geschichte um den misstrauischen Vater und den technisch versierten Freund seiner Tochter hatte noch eine weitere Komponente mit justiziellen Folgen. Der junge Mann hatte offenbar Kontakt zur No-Name-Crew, einer anonymen Gruppe von Hackern und InternetaktivistInnen, die zum Ziel hat, gegen staatliche Eingriffe im Internet vorzugehen. Dabei bedient sie sich zumindest fragwürdiger Methoden. Bei der Staatsanwaltschaft Köln ist seit Sommer 2011 ein Verfahren anhängig. Der junge Mann aus Frankfurt bot die heruntergeladenen Kommunikationspläne der No-Name-Crew an. Ob die Gruppe Interesse hatte, ist unklar. Doch alleine der Kontakt zwischen dem Hacker und den Aktivisten führte dazu, dass sich die Kölner Staatsanwälte einschalteten. Deren Pressesprecher erhielt nach Bekanntwerden des Falls vorwiegend aus dem Rhein-Main-Gebiet Presseanfragen. Die Bundespolizei hatte zuvor verlauten lassen, die Kölner Staatsanwaltschaft werde sich zu dem Fall äußern, was aber nicht zutraf. Um die Ermittlungen in dem Verfahren gegen die No-Name-Crew nicht zu gefährden, könne er in der Angelegenheit des Frankfurter Bundespolizisten „keinerlei Auskunft" geben. Die Wortkargheit erklärt sich damit, dass die No-Name-Crew im Juli 2011 eine spektakuläre Aktion gestartet hatte, als sie den sogenannten Patras-Server angegriffen hatte, ein GPS-Fahndungssystem, mit dem Zoll und Polizei den Standort von Verdächtigen orten können (vgl. DANA 3/2011, 114). Mit der Attacke auf „Patras" habe der junge Mann, der dem neugierigen Vater die Daten stahl, nichts zu tun, hieß es von der Bundespolizei (www.fr-online.de 09.01.2012; Der Spiegel 2/2012, 14).

Mecklenburg-Vorpommern

Professor praktiziert Prüfungsvideoüberwachung

Ein Rostocker Mathematikprofessor nutzte Videokameras zur Überwachung von 120 Studierenden bei einer Prüfung. Da dies unzulässig ist, besteht nun das Risiko, dass Betroffene die Prüfung annullieren lassen. Der Professor gab zu: „Das war mein Fehler." Er habe nicht gewusst, dass das Verfahren bei Prüfungen nicht zulässig ist. Der Prüfungsraum, ein Audimax, sei zu unübersichtlich gewesen, um nur durch einen Prüfenden beaufsichtigt zu werden. Die Universität war zunächst für eine Stellungnahme nicht zu erreichen (SZ 20.02.2012, 9).

Nordrhein-Westfalen

Massenhafte polizeiliche Handyordnung mit „stiller SMS"

Der NRW-Innenminister Ralf Jäger (SPD) nannte auf eine Kleine Anfrage der Linken-Landtagsabgeordneten Anna Conrads Details zur Handy-Überwachung: Danach wurden 2010 2.644 Mobiltelefone heimlich mit „stillen SMS" geortet. Hintergrund der Anfrage war die heimliche Handy-Ortung der Polizei in Sachsen per Funkzellenabfrage anlässlich Antifaschistischer Demonstrationen im Februar 2011 (DANA 3/2011, 119 ff.). Danach scheint die polizeiliche Handy-Ortung längst ein Standardverfahren und keine Ausnahme mehr zu sein.

Zum Einsatz der Funkzellenauswertung sagte Innenminister Jäger nicht viel. Er verwies lediglich auf Paragraf 100g der Strafprozessordnung (StPO), nach dem die Maßnahme nur auf richterliche Anordnung und bei Verdacht auf Straftaten von erheblicher Bedeutung erlaubt ist. Wie oft diese Überwachungstechnik eingesetzt wurde, vermöge er nicht zu sagen, da die Funkzellenauswertung ein „Unterfall der in § 100g StPO normierten Verkehrsdatenerhebung" sei und „nicht selbständig in der Statistik erfasst" werde. Bzgl. der „Ortungsimpulse" wurde Jäger dagegen konkreter. Demnach wurden im vergangenen Jahr in 776 Ermittlungsverfahren insgesamt 5.276 Mobiltelefone überwacht. An rund die Hälfte davon, nämlich an 2.644 Geräte, wurden Ortungssignale versandt. Um ein Handy zu orten oder den Weg eines Handybesitzes nachzuzeichnen, müssen zum Teil Hunderte Signale versandt werden. Die Gesamtzahl der im Jahr 2010 versandten Ortungssignale lag deshalb bei 255.784. Damit war in Nordrhein-Westfalen die Zahl zum ersten Mal seit Jahren gesunken. Zwischen 2006 und 2009 war sie kontinuierlich von rund 156.000 auf ziemlich genau 320.000 gestiegen. Jäger konnte nicht sagen, wie

viele Ermittlungsverfahren und wie viele betroffene Anschlüsse in diesen Jahren diesen Zahlen zuzuordnen sind. Außerdem sagt die Zahl allein nichts darüber aus, wie oft jemand wirklich geortet wurde. Denn ein Ortungssignal „an ein Endgerät, das nicht betriebsbereit war (z. B. ausgeschaltet) oder im Ausland betrieben wurde“, hat keinen Effekt. Er nannte drei Beispiele für einen erfolgreichen Einsatz der Technik, wohl um den tausendfachen Einsatz zu rechtfertigen: Ein flüchtiger Gewaltverbrecher, ein Vergewaltiger und ein Drogendealer hätten mit Hilfe von Ortungssignalen gefasst werden können (Beuth www.zeit.de 23.11.2011; zur „stillen SMS“ auf Bundesebene siehe oben S. 21).

Rheinland-Pfalz

Polizeikennzeichnung in der Diskussion

In Rheinland-Pfalz sollen - ähnlich wie in Berlin (DANA 1/2011, 19) - die PolizistInnen bei Fußballspielen oder Demonstrationen künftig eine besondere Kennzeichnung tragen, wobei ein rotierendes Nummernsystem erwogen wird. Die Gewerkschaft der Polizei (GdP) im Lande lehnt die Identifizierung per Namensschild bei Großeinsätzen ab, so wie sie bisher bei StreifenpolizistInnen praktiziert wird. GdP-Landeschef Ernst Scharbach warnte, dass für Beamte mit Namensschildern gerade bei riskanten Einsätzen ein „erhebliches Bedrohungspotenzial“ bestehe (SZ 31.01.2012, 6).

Thüringen

Lutz Hasse ist neuer Landesdatenschutzbeauftragter

Am 24.02.2012 wurde Dr. Lutz Hasse mit 45 Stimmen (erforderlich waren 44) zum neuen Thüringer Landesbeauftragten für den Datenschutz gewählt. Constanze Kurz, die gegen ihn auf Vorschlag der Fraktion der Grünen kandidierte, erhielt 34 der 82 abgegebenen gültigen Stimmen. Der 52jährige Jurist Hasse, der zuletzt als Referatsleiter im Thüringer Ministerium für Soziales, Familie und Gesundheit tätig war, übernahm am 01.03.2012 die Aufgabe von Harald Stauch, der das Amt seit 2006 inne hatte. CDU-Fraktionschef Mike Mohring und SPD-Kollege Uwe Höhn hatten sich nach einigem Hin und Her auf Hasse geeinigt. Lutz Hasse hatte zuvor für einige Zeit unter seinem Vorgänger Stauch gearbeitet.

Die oder der Landesbeauftragte muss mit der Mehrheit der Stimmen des Landtags gewählt werden. Eine einmalige Wiederwahl ist zulässig. Die Vorschläge kommen von den einzelnen Fraktionen, die auch die Mehrheiten für ihren Kandidaten organisieren müssen. Vor der Novellierung des Landesdatenschutzgesetzes (LDSG) Ende 2011 hatte die Landesregierung das alleinige Vorschlagsrecht für den Kandidaten. Der Posten ist mit der Besoldungsgruppe 6 ausgezeichnet. Das Brutto-Jahreseinkommen liegt bei etwa 95.000 Euro und ist damit höher als in fast allen anderen Bundesländern. Seit Ende 2011 ist zur Kontrolle des öffentlichen Bereichs die Aufsicht über die Privatwirtschaft hinzugekommen. Hier können auch Bußgelder verhängt werden.

Man kann nicht sagen, dass der 58jährige Vorgänger Stauch sich in seinem Amt allzu kritisch betätigt hätte. Stauch ist gelernter Diplomingenieur und war von 1990 bis 2006 Mitglied des Thüringer Landtags, seit 1994 parlamentarischer Geschäftsführer der CDU-Landtagsfraktion. Doch übte er sein Datenschutzamt offensichtlich dennoch zu unabhängig aus, wagte er es doch ab und zu, sich kritisch gegenüber der Regierung zu äußern, zuletzt bei der völlig missglückten LDSG-Überarbeitung im Jahr 2011. In seinem letzten Tätigkeitsbericht hatte Stauch Kommunen, Polizei und Schulverwaltungen kritisiert und sich unter anderem gegen ausufernde Videoüberwachung und gegen Funkzellenabfragen ausgesprochen. Für Union und SPD kam er deshalb scheinbar für weitere sechs Jahre nicht infrage. Beide Fraktionen stritten sich anschließend lediglich darum, wer denn nun einen Nachfolger vorschlagen dürfe. Die Ablösung als Datenschutzbeauftragter des Freistaats Thüringen kam für Stauch überraschend. Im Vorfeld hatte keiner mit ihm darüber gesprochen. Er berichtete gegenüber der Presse, dass er „Quasi auf der Skipiste“ erfuhr, dass die Regierungsfraktionen von CDU und SPD bereits munter über einen Nachfolger reden: „So wie das offenbar gelaufen ist, lässt es den Respekt vor dem Amt des Datenschutzbeauftragten vermissen“. Er habe nie freiwillig auf eine Kandidatur an der Spitze der Behörde verzichtet.

Die Grünen hatten überraschend eine kompetente Gegenkandidatin präsentiert: Constanze Kurz ist Mitglied der Enquete-Kommission Internet und digitale Gesellschaft des Deutschen Bundestages sowie Sprecherin des Chaos Computer Clubs. Am 21.02.2012 hatten die Grünen in ihren Fraktionsberatungsraum eingeladen. Mitglieder der Piratenpartei, Anhänger der Linken aber auch junge ComputerexpertInnen waren gekommen, um Constanze Kurz kennenzulernen. „Wir sind für eine freie Internetkultur“, sagte Fraktionschefin Anja Siegesmund zu Beginn der Diskussionsrunde. Gleichzeitig müsse die Datensammelwut von Behörden und der Wirtschaft eingedämmte werden. Constanze Kurz erklärte, dass sie sich gerne bereit erklärt habe, für das Amt zu kandidieren. Datenschutz sei in den vergangenen Jahren immer politischer geworden, die BürgerInnen hätten immer mehr Fragen dazu. Sie betonte, das Amt sei zu wichtig, um es an einen Proporzkandidaten der Parteien zu vergeben. Constanze Kurz räumte ein, dass ihr bewusst sei, dass die Chance auf ihre Wahl nicht riesig sei. Sie würdigte die Tätigkeit des bisherigen Thüringer Datenschutzbeauftragten Harald Stauch; er habe eine gute Arbeit abgeliefert.

Dem freundlichen Empfang durch die Linken gegenüber Constanze Kurz war allerdings ein Angriff von Linkenfraktionschef Bodo Ramelow auf die Grünen vorausgegangen. In einem Radio-Interview warf er der kleineren Fraktion vor, dass diese überhaupt kein Vorschlagsrecht für die Neubesetzung des Landesdatenschutzbeauftragten habe. Erst später wurde ihm klar, dass das LDSG geändert worden war und nun nicht mehr die Landesregierung, sondern das Parlament Vorschläge unterbreiten darf. „Ich habe mich für den Fehler bei Anja Siegesmund entschuldigt“, erklärte Bodo Ramelow und kündigte an, die Kandidatin der Grünen unterstützen zu wollen. Immerhin sitze Constanze Kurz für die Linken als Sachverständige in der Enquete-Kommission „Internet und digitale Gesellschaft“ des Bundestages.

Landtagspräsidentin Birgit Diezel (CDU) gratulierte dem neu gewählten Datenschutzbeauftragten: „Dr. Hasse besitzt durch seine Beschäftigung beim Datenschutz eine langjährige Erfahrung auf diesem Gebiet. Durch seine Tätigkeit als Referatsleiter beim Thüringer Datenschutzbeauftragten weiß er um die zukünftigen Herausforderungen. Ich wünsche Dr. Hasse, dass er mit Engagement die neue Tätigkeit beginnen wird. Für die neuen Herausforderungen wünsche ich ihm viel Erfolg.“ Sie dankte dem aus dem Amt scheidenden Stauch. Dieser habe sich der komplexen Materie Datenschutz engagiert angenommen und gemeinsam mit seinen Mitarbeitern nicht nur für die Einhaltung der Datenschutzrichtlinien gesorgt, sondern auch das Bewusstsein der Behörden und der Öffentlichkeit für den Datenschutz sensibilisiert. „Für diese geleistete Arbeit bin ich sehr dankbar. Seine Amtszeit ist von stetigem Engagement geprägt. Ich danke Harald Stauch für die geleistete Arbeit, die er mit so viel Engagement betrieben hat. Sein Nachfolger kann auf einem guten und sicheren Fundament aufbauen.“

Derzeit arbeiten 12 Mitarbeitende in der Behörde, die ihren Sitz im Thüringer Landtag in der Jürgen-Fuchs-Str. 1 hat. Insgesamt ist das Haus in drei Referate aufgeteilt - zwei beschäftigen sich vorrangig mit Rechtsthemen und Rechtsproblemen, das dritte Referat kümmert sich um anfallende Technikfragen (Rathay/Mudra www.thueringer-allgemeine.de 22.02.2012; Biermann www.zeit.de 24.02.2012; PM Thüringer Landtag 24.02.2012).

Datenschutznachrichten aus dem Ausland

Europa

Mosley klagt gegen Sadomaso-Bilder im Netz

Der frühere 71jährige Motorsport-Präsident Max Mosley will neben Google weitere Suchmaschinenbetreiber verklagen, um Fotos einer privaten Sadomaso-Party aus dem Internet zu tilgen: „Wenn wir gegen Google vor Gericht gewinnen, wird es wohl nicht mehr nötig sein, andere zu verklagen. Aber wenn es notwendig ist, machen wir es.“ Mosley klagt in Frankreich und Deutschland, weil das Unternehmen über seine Internetbildersuche immer wieder Fotos anzeigt, die in diversen Gerichtsverfahren als illegaler Eingriff in die Intimsphäre eingestuft wurden. Als Verhandlungstermin vor dem Landgericht (LG) Hamburg war der 30.03.2012 vorgesehen. Mosley, britischer Staatsbürger, will erreichen, dass Google sich verpflichtet, die Fotos gar nicht erst in seinen Suchergebnissen anzuzeigen. Es geht konkret um 10 Bilder, die Mosley mit 5 Frauen zeigen. 2008 hatte das inzwischen eingestellte Skandalblatt „News of the World“ (siehe unten S. 29) Mosley bei einer Sexparty gefilmt und die Fotos im Netz veröffentlicht.

Allein in Deutschland hat Mosley erwirkt, dass 190 Internetseiten mit Fotos gelöscht werden mussten. Die Bilder tauchten jedoch immer wieder auf Seiten auf, deren Betreiber oft nicht ermittelbar waren. Google argumentiert, es könne keine Bilder sperren, solange kein Urteil gegen einen Betreiber vorliege; alles andere sei Zensur. Das Unternehmen sieht sich nicht verantwortlich für den Inhalt von Webseiten, hat allerdings nach Aufforderung von Mosleys Anwältin in Deutschland, Tanja Irion, einzelne Bilder entfernt: „Nach welchen Kriterien Google entscheidet, wann sie löschen und wann nicht, ist uns nicht ersichtlich. Das ist Willkür.“ Mosley erklärte, er halte es für „falsch und erniedrigend“, dass er immer wieder bei Google die nachträgliche Löschung der Bilder beantragen müsse. Er will den Ausgang der Verfahren in Europa abwarten, bevor er eine Klage gegen Google in Kalifornien/USA prüft (Der Spiegel 49/2011, 167).

Europa

USA beanspruchen Mitspracherecht bei EU-Datenschutzreform

In der Debatte über die Reform des Datenschutzrechts in Europa meint die US-Regierung, Teil des Reformprozesses zu sein. Der oberste Jurist des US-Handelsministeriums, Cameron F. Kerry, sagte am Mittwoch in Berlin: „Wir verstehen die internationalen Partner als Beteiligte im internationalen Prozess und andersherum verstehen wir uns als Beteiligte im europäischen Prozess.“ Die EU-Justizkommissarin Viviane Reding hatte sich in Brüssel über die Versuche der Einflussnahme sowohl von Firmen als auch Regierungsinstitutionen aus anderen Ländern schon vor der Veröffentlichung der ersten Entwürfe beklagt.

Kerry war nach einer Visite in Brüssel, wo er mit Vertretern des Europaparlaments, der Presse und der EU-Kommission zusammentraf, in Berlin, um dort unter anderem mit dem Bundesdatenschutzbeauftragten Peter Schaar zu reden. Hintergrund der Europareise waren neben der Datenschutzreform die gerade von der US-Regierung vorgestellten Regelungen für Datenschutz, die auf US-Bundesstaatsebene Mindestkriterien für den Datenschutz festlegen und Verbrauchern und der Handelsaufsicht FTC rechtliche Werkzeuge zur Durchsetzung an die Hand geben sollen.

Kritiker bezeichnen den Vorstoß des Weißen Hauses als vergleichsweise schwach. Kerry hingegen betonte, dass Europa vor allem auf dem Papier ein starkes Datenschutzrecht habe, während in den USA das tatsächliche Niveau der Durchsetzung beachtlich sei. Datenschutz sei in den USA ein wichtiges Thema geworden.

Bedenken wegen Zugriffsmöglichkeiten für US-Nachrichtendienste auf Daten, die in den USA gehalten oder von dortigen Unternehmen kontrolliert werden, wie es der Patriot Act

vorschreibt, wies Kerry zurück: Das Gesetzespaket sei diesbezüglich in erster Linie „ein Monster unter dem Bett“. Unter anderem die mangelnden Rechtsschutzmöglichkeiten für Nicht-US-Bürger hatten immer wieder Kritik ausgelöst – die Kerry für überzogen erklärte. In Wahrheit wären die Zugriffsmöglichkeiten für staatliche Stellen in Europa viel weitergehender als die der US-Behörden. (Falk Lüke, http://www.heise.de/newsticker/meldung/USA-beanspruchen-Mitspracherecht-bei-EU-Datenschutzreform-1445922.html)

Niederlande

Kameragrenzkontrolle zu Deutschland und Belgien

Die Niederlande führten zum Jahreswechsel 2011/2012 an allen großen Grenzübergängen zu Deutschland (10) und Belgien (5) automatische Grenzkontrollen ein, bei denen Kameras Kfz und LKW fotografieren. Hinzu kommen 6 mobile Kameras, die an kleineren Übergängen eingesetzt werden. Fällt hierbei ein verdächtiges Auto auf, so wird es kurz darauf von einer Polizeistreife gestoppt. Justizminister Ivo Opstelten erläuterte, hierdurch könne man z. B. Kleinbusse aus Bulgarien und Rumänien abfangen, die Zwangsprostituierte ins Land bringen. Das eingesetzte System heißt „@migo-boras“ und basiert auf einer Nummernschilderkennung (automatic number plate recognition - ANPR). Mit welchen Datenbeständen die fotografierten Nummernschilder abgeglichen werden, ist bisher nicht klar. Das Projekt wurde zunächst als Pilotprojekt begonnen und sollte im Frühjahr 2012 offiziell starten. Laut Immigrationsminister Gerd Leers ermöglicht die Erfassung die Aufzeichnung von „Verkehrsmustern“, die „auf Basis allgemeiner Daten und Zielgruppenprofilen melden, welches Fahrzeug für eine Kontrolle interessant sein kann“. Die gewonnenen Informationen würden umgehend der Grenzpolizei übermittelt, die dann das entsprechende Auto anhalten kann. Gemäß einem Gesetzentwurf der Regierung in Den Haag sollen die Daten vier Wochen lang gespeichert werden dürfen. Sie sollten nicht dazu genutzt werden, säumigen ParksünderInnen auf die Spur zu kommen, so ein Sprecher des Innenministeriums: „Dies ist ein Instrument gegen schwere Kriminalität wie Menschenhandel, es eignet sich überhaupt nicht, um ausstehende Geldbußen zu kassieren.“

Niederländische DatenschützerInnen kritisieren das Vorhaben. Die Stiftung Privacy First spricht von einem „enormem Eingriff in die Privatsphäre“. Alle Fahrzeuge zu kontrollieren, um bei einem etwas Verdächtiges zu finden, sei eine „Umkehrung des Rechtssystems“. Die Datenschutz-Website sargasso.nl befürchtet, die Grenzpolizei habe damit zumindest die Möglichkeit, einreisende Autos gleichzeitig mit „allerlei schwarzen Listen“ abzugleichen. Eben dies verneint Immigrationsminister Leers entschieden. Ebenso wenig würden die gewonnenen Informationen gespeichert; immerhin gesteht er ein: „Wohl können die Kameras anhand des Kennzeichens sehen, aus welchem Land ein Auto oder LKW kommt.“

Herbst 2011 begann sich die EU-Kommission für den Fall zu interessieren. Nachdem Deutschland aus Sorge um den freien Verkehr zwischen den Mitgliedsstaaten in Brüssel eine Klage eingereicht hatte, wandte sich EU-Innenkommissarin Cecilia Malmström mit der Bitte um mehr Informationen an die Regierung in Den Haag. Der kritische Blick aus Brüssel erklärt sich nicht zuletzt aus dem Kontext des letzten Jahres. Sowohl Frankreich als auch Dänemark führten 2011 vorübergehend Grenzkontrollen ein, was in anderen Mitgliedsstaaten grundsätzliche Diskussionen auslöste. Dabei ging es auch um eine mögliche Signalwirkung: Grenzpolitische Alleingänge einzelner Mitglieder könnten die Erosion europäischer Errungenschaften wie beispielsweise den Wegfall der Binnengrenzen zur Folge haben. Die EU-Kommission will prüfen, ob die Kameras an der Grenze gegen das Schengen-Abkommen des freien Grenzverkehrs verstoßen. Wie in Dänemark, das teilweise Grenzkontrollen wieder einführte, gelten auch in Holland die Rechtspopulisten als treibende Kraft hinter den Kontrollen an den Außengrenzen. Ein Sprecher des holländischen Grenzschutzes rechtfertigt diese: „Im Grunde tun die Kameras dasselbe wie die Kollegen, die an der Autobahn stehen und Autos herauswinken.“

Frank Richter, der stellvertretende Bundesvorsitzende der deutschen Gewerkschaft der Polizei (GdP), meinte: „Wir lehnen eine permanente Überwachung konsequent ab.“ Ein solches System dürfe nur kurzfristig bei einer aktuellen Fahndung eingesetzt werden. Für die Niederlande sind die Fotokameras an den Grenzen nur der Ausbau eines Überwachungssystems, das im Inland schon an den meisten Autobahnen installiert ist und die Autos der Vorbeifahrenden fotografiert. Im einst liberalen Land gibt es darüber keine große Diskussion mehr (Dörries SZ 30.11.2011, 6; Müller www.zeit.de 04.01.2012).

Luxemburg

YouPorn-Chatter im Internet geoutet

Unbekannte haben 6.000 NutzerInnen-Namen und Passwörter von Teilnehmenden des YouPorn-Chats veröffentlicht. Damit gerät die YouPorn-Mutterfirma Manwin mit Sitz in Luxemburg bereits das zweite Mal innerhalb weniger Tage negativ in die Schlagzeilen. Im Netz veröffentlicht wurden E-Mail-Adressen und Passwörtern. Es kursiert eine Liste mit etwa 6.400 Datensätzen. Der schwedische Sicherheitsblogger Anders Nilsson berichtete sogar von einer Million betroffener Registrierungen, doch wurden seine Angaben nicht verifiziert. YouPorn zufolge handelt es sich nicht um die Informationen über die Nutzenden, die sich nur bei dem Portal selbst angemeldet haben. Betroffen sind offenbar lediglich Mitglieder des YouPorn-Chats, der von einer anderen Firma betrieben wird und dessen Daten damit auch auf einem anderen Server gespeichert wurden. Nilsson zufolge soll diese Fremdfirma seit 2007 fahrlässig mit den Login-Daten des Chats umgegangen sein: So seien die Informationen unverschlüsselt gespeichert worden und über eine öffentliche URL zugänglich gewesen sein. Kreditkartendaten hatten die Nutzenden offenbar nicht hinterlegt.

YouPorn hat den Chat inzwischen abgeschaltet, betont aber, für die 4,75 Millionen regulär angemeldeten User bestehe keine Gefahr, sofern sie sich nicht für das Chatforum registriert hätten. Bereits eine Woche zuvor war die YouPorn-Mutterfirma Manwin in die Schlagzeilen geraten, als ein unbekannter Hacker Nutzernamen, E-Mail-Adressen und verschlüsselte Passwörter des Manwin-Sexportals Brazzers im Netz veröffentlicht und behauptet hatte, insgesamt 350.000 Datensätze zu besitzen. Auch hier waren keine Kreditkarteninformationen betroffen. Manwin hatte angekündigt, die NutzerInnen mit kostenlosen Brazzers-Zugängen zu entschädigen (www.sueddeutsche.de 23.02.2012).

Frankreich

Prominenter Staatsanwalt soll Journalisten bespitzelt haben

Der bekannte Staatsanwalt Philippe Courroye wurde am 17.01.2012 von einer Untersuchungsrichterin einbestellt, um die Einleitung eines Ermittlungsverfahrens mitgeteilt zu bekommen, weil er Journalisten der Zeitung „Le Monde“ ausspioniert habe. Es steht die Behauptung im Raum, dies sei auf Wunsch des Élysée-Palastes erfolgt, was jedoch das Präsidialamt bestreitet. Courroye wurde bekannt durch unerschrockene Ermittlungen gegen Francois Mitterrands Sohn Jean-Christoph und den gaullistischen Spitzenpolitiker Charles Pasqua. Nun muss er sich verteidigen gegen den Vorwurf, „auf unerlaubte, unlautere und betrügerische“ Weise private Daten ermittelt und das Kommunikationsgeheimnis verletzt zu haben. Der 52jährige Staatsanwalt sieht sich nun als Opfer „mörderischer Attacken“ und einer „Menschenjagd“. Im Jahr 2010 führte Courroye Ermittlungen im Fall Liliane Bettencourt, in dem es u. a. darum ging, ob die Milliardärin Steuern hinterzogen und illegale Spenden an die UMP-Partei von Präsident Nicolas Sarkozy geleistet hat. Da Le Monde verblüffend gut über Details des Verfahrens informiert war, wollte Courroye herausfinden, aus welchen Quellen das Blatt schöpfte. Es ließ ermitteln, mit wem drei Journalisten telefoniert oder SMS ausgetauscht hatten. Als Quelle verdächtigt wurde eine Richterin, mit der Courroye verfeindet ist.

Le Monde sieht in der Bespitzelung eine Verletzung des Quellenschutzes und stellte Strafantrag. Bereits im Oktober 2011 leitete die Justiz ein Ermittlungsverfahren gegen den Chef des Inlandsgeheimdienstes, Bernard Squarcini, ein. Im Dezember entschied der oberste Gerichtshof in Paris, die Sammlung der Telefondaten sei rechtswidrig gewesen. Nun muss Courroye mit strafrechtlichen Konsequenzen rechnen. Kritiker werfen dem ehrgeizigen Staatsanwalt vor, im Amt den Interessen Sarkozys zu dienen. Er habe in diversen Verfahren Gefolgsleute des Präsidenten geschützt und auch in der Bettencourt-Affäre versucht, Schaden von Sarkozy abzuwenden. Der Beschuldigte bestreitet eine ungebührliche Nähe zum Präsidenten. Sarkozy selbst sagte, als er Courroye 2009 mit dem hohen Orden „Légion d´honneur“ auszeichnete: „Man wirft uns vor, einander zu kennen und sogar zu schätzen. Aber wären wir unabhängiger, wenn wir verfeindet wären?“ Courroye hat Einspruch gegen das Ermittlungsverfahren eingelegt. Er rechtfertigt sich damit, lediglich Telefonverbindungsdaten, nicht aber den Inhalt von Gesprächen und SMS ausgeforscht zu haben. Damit sei der Quellenschutz nicht verletzt. Die Anwälte von Le Monde sehen das anders und fordern die gerichtliche Klärung, wie weit sich JournalistInnen auf den Schutz ihrer Quellen verlassen können. Courroye konterte mit einem Zitat des Revolutionspolitikers Graf von Mirabeau: „Die Zeit, dieser unbestechliche Richter, lässt allen Gerechtigkeit zuteil werden“ (Ulrich SZ 10.01.2012, 7).

Großbritannien

Rupert Murdoch schließt Vergleiche mit 36 Abhöropfern

Im „News-of-the-World“-Abhörskandal hat sich Medienmogul Rupert Murdoch bzw. dessen Unternehmen „News International“ (NI) am 19.01.2012 mit Dutzenden Opfern auf Vergleiche geeinigt (vgl. DANA 2/2012, 86 f.). Die Opfer erhalten nach Presseangaben insgesamt 645.000 Pfund (ca. 750.000 Euro). Dazu kommen Anwaltskosten, die um ein Vielfaches höher liegen dürften. Zu den Abhöropfern gehören Schauspieler Jude Law, Fussballspieler Ashley Cole und der ehemalige britische Vize-Premier John Prescott. Murdochs britisches Verlagsunternehmen News Group Newspapers, dem das inzwischen wegen der Abhöraktion eingestellte Boulevard-Blatt „News of the World“ gehörte, einigte sich bei einer Anhörung vor dem High Court in London mit den Opfern. Nach Angaben von Opferanwälten erhielt Law die höchste Summe, nämlich 130.000 Pfund Entschädigung. Die hohe Einzelsumme liegt daran, dass Laws Telefon auch gehackt wurde, als dieser sich in den USA befand. Die NI-Anwälte befürchteten wohl eine Klage in den USA, wo der Vergleich vermutlich nicht so billig ausgefallen wäre. Law erklärte, ihm ginge es nicht ums Geld, sondern um die Wahrheit. Nun, da der Fall gerichtlich abgeschlossen sei, könne er sich endlich äußern.19 Opfer ließen im Gericht Statements verlesen. Laws Anwalt schilderte für seinen Mandanten: „Kein Aspekt meines Privatlebens war sicher.“ Seine Kinder und seine Mitarbeitenden seien bespitzelt worden, sein Haus permanent beobachtet und er konstant verfolgt. Obwohl er seine Handys fortlaufend wechselte und sein Haus auf Wanzen überprüfen ließ, gelangten private Informationen in die Murdoch-Presse: „Ich fing an, denen zu misstrauen, die mir nahestanden.“

News Group Newspapers gab zu, zwischen 2003 und 2006 insgesamt 16 Artikel über Law in der „News of the World“ veröffentlicht zu haben, die auf über Abhörmaßnahmen erlangten Informationen basierten. Zudem sei der Schauspieler physisch überwacht worden, und zwar „wiederholt und anhaltend“. Der Verlag gab ebenfalls zu, dass „The Sun“ illegal erlangte Informationen über Laws Privatleben genutzt hat, machte aber keine weiteren Angaben. Laws Anwalt erklärte vor Gericht, das Vorgehen der Boulevardzeitung habe „erheblichen Kummer, Misstrauen und Argwohn“ verursacht. Frost erklärte, sie und Law hätten begonnen, einander zu misstrauen. Law war einer von

60 Menschen, die gegen den Murdoch-Konzern geklagt haben.

Den Aspekt „Misstrauen" betonten viele Opfer. Da sie sich nicht erklären konnten, wie die privatesten Informationen an die Öffentlichkeit gelangten, beschuldigten sie Freunde und Familie. Die Schauspielerin Sienna Miller erzählte zuvor einem Untersuchungsausschuss, wie sie zwei Verwandte und zwei Freunde zusammenrief und schwer beschuldigte, und wie sie sich heute schäme, ihnen misstraut zu haben. Neben Law wurde mit 35 weiteren Opfern eine Vergleichszahlung vereinbart. Sie erhielten im Schnitt mehrere zehntausend Pfund. So soll Laws Ex-Frau, die Schauspielerin Sadie Frost, 50.000 Pfund Entschädigung erhalten. Auch der frühere Geliebte der verstorbenen Prinzessin Diana, James Hewitt, die australische Sängerin Dannii Minogue und der walisische Rugbystar Gavin Henson sowie Schauspielerin Sienna Miller werden vom Murdoch-Konzern entschädigt, ebenso wie der Fußballer Ashley Cole, der ehemalige Vizepremier John Prescott, verschiedene Parlamentsabgeordnete und ein anonymer Mann, der überwacht wurde, weil er mit einer Prominenten liiert war.

Nach jeder Erklärung erhob sich der Anwalt von News Group und entschuldigte sich im Namen des Unternehmens für die durch die illegalen Aktivitäten verursachten Schaden und Kummer. Die Vergleichssummen kommen aus einem Entschädigungstopf, den NI nach dem Abhör-Skandal eingerichtet hat. Der Medienkonzern möchte sich mit den Abhör-Opfern außergerichtlich vergleichen und so kostspielige Prozesse vermeiden. Im Juli 2011 war herausgekommen, dass Journalisten der „News of the World" jahrelang Handymailboxen von Prominenten und Angehörigen getöteter Soldaten sowie von Kriminalitätsopfern abgehört hatten. Die Affäre führte nicht nur zur Einstellung des Blatts, sondern auch zum Rücktritt von Vertrauten Murdochs und hoher Polizisten. Auch Premier David Cameron geriet unter Druck, weil er den ehemaligen „News of the World"-Chefredakteur Andy Coulson als Sprecher beschäftigt hatte. Für Rupert Murdoch und NI ist die Sache noch längst nicht erledigt. Laut Scotland Yard wurden 800 Personen systematisch abgehört. Insgesamt gibt die Polizei an, dass „News of the world" die Telefone von 5.795 Menschen abgehört hat. Sie alle könnten Geld von Murdochs Konzern fordern (Zaschke SZ 09.12.2011, 17; www.persoenlich.com 19.01.2012; Zaschke SZ 20.01.2012, 15).

Großbritannien

Ziviler Streifenpolizist jagte sich per Videofahndung selbst

Im Januar 2012 jagte sich in der südenglischen Grafschaft Sussex ein Polizist mit Hilfe von Kameras für etwa 20 Minuten selbst. Sein Kollege an den Monitoren hatte ihn nicht erkannt und fand sein Verhalten sehr auffällig. Der beobachtete Mann verhalte sich dringend tatverdächtig. Er gab seinem Kollegen in Zivil per Funk durch, er habe jemanden gesichtet, der sich auffällig benahm. Leider bemerkte der Polizist auf Probe nicht, dass er dabei seinen eigenen Kollegen ins Visier genommen hatte. Dem Mann auf Fußstreife wurde mitgeteilt, der Verdächtige würde sich sehr schnell bewegen. Der Polizist an den Monitoren nahm an, ein mutmaßlicher Täter befände sich nach getätigtem Einbruch in einem der Läden der Stadt auf der Flucht. Die Geschwindigkeit des Mannes war nicht verwunderlich, denn der Läufer war der Zivilermittler höchst selbst. Es dauerte etwa zwanzig Minuten, bis sein Vorgesetzter den Kontrollraum betrat, den angeblichen Täter erkannte und hysterisch zu lachen begann. So klärte sich auch, weshalb der Streifenpolizist den Flüchtigen trotz der Funkdurchsagen seines Kollegen nie sehen konnte. Die „Operation Fehltritt" wurde von einem Polizeimagazin veröffentlicht, welches die näheren Umstände und die Namen der Beteiligten zu deren Schutz verschwieg. Der Vorgesetzte wird damit zitiert, der neue Kollege sei wohl etwas übereifrig gewesen. Dennoch sei er froh über jede Gelegenheit, wenn er bei seinem anstrengenden Beruf auch mal einen Grund zum Lachen habe (Sobiraj www.gulli.com/news/18091 09.02.2012).

Griechenland

Internetpranger für Steuersünder

Das griechische Finanzministerium in Athen hat nach längerer Vorwarnung und Debatten zum Datenschutz am Abend des 22.01.2012 eine 100 Seiten lange Liste der SteuersünderInnen des Landes ins Internet gestellt unter Angaben von 4.152 Namen und den jeweiligen Summen von deren Steuerschuld. Die vom Finanzminister Evangelos Venizelos „Liste der Schande" genannte Aufzählung beginnt mit einem gewissen Nikolaos Kasimatis, zu dem 952.087.781,55 Euro Schulden angegeben sind. Zu den schwarzen Schafen gehören KünstlerInnen, UnternehmerInnen, Geschäfts- und Privatleute. Ganz große Namen sind nicht zu finden. Die Regierung hatte den SchuldnerInnen am 14.11.2011 eine zehntägige Frist gesetzt zur Begleichung der Außenstände bei den Finanz- und Zollämtern. Zudem wurden in den vorangegangenen zwei Monaten ca. 90 zum Teil prominente UnternehmerInnen festgenommen, die dem Staat beachtliche Summen schulden. Mit diesen spektakulären Aktionen wollten die Behörden offensichtlich nach langer Untätigkeit Entschlossenheit demonstrieren.

Die auf der „Liste der Schande" aufgeführten Beträge summieren sich auf knapp 15 Mrd. Euro. Einige der Genannten sitzen bereits im Gefängnis; betroffene Unternehmen sind insolvent oder in Prozesse verwickelt. In Griechenland sollen 165.000 Steuerverfahren vor den Gerichten anhängig sein. Die „Task Force Griechenland", die im Auftrag der EU-Kommission der Regierung in Athen bei der Bürokratiereform helfen soll, hat die ausstehenden Steuern aus den vergangenen Jahren auf 60 Mrd. Euro beziffert. Eingerechnet sind dabei aber auch die extrem hohen Strafen, die in Griechenland verhängt werden, wenn eine Steuerhinterziehung bekannt wird. Ein großes Problem lag bisher in der teilweisen Unfähigkeit und Unwilligkeit, Steuern und Abgaben einzutreiben. Hierzu fehlt es auch am nötigen Werkzeug. Die Datenverarbeitung steckt in diesem Bereich in den Kinderschuhen (Schlötzer SZ 24.01.2012, 2).

Tschechien

Verfassungsgericht verwirft erneut Vorratsdatenspeicherung

Das Verfassungsgericht der Tschechischen Republik hat am 04.01.2012 erneut ein Urteil gegen die Vorratsdatenspeicherung gesprochen. Bereits im März 2011 hatte das oberste Gericht das dortige Umsetzungsgesetz der EU-Richtlinie annulliert und damit die Verpflichtung der Provider zur sechsmonatigen Speicherung der Daten aufgehoben. Wie in Deutschland speichern einige Provider Verbindungs- und Bewegungsdaten weiter, auch wenn diese nicht für Rechnungszwecke benötigt werden. Im aktuellen Urteil wurde § 88a der tschechischen Strafprozessordnung annulliert, worin geregelt war, wie diese Daten zu Ermittlungen übermittelt und verwendet werden dürfen. Das erscheint dem Gericht zu allgemein sowie nicht verhältnismäßig und damit verfassungswidrig. Die Regelung verstoße auch gegen das Recht auf Privatsphäre und informationelle Selbstbestimmung (Meister netzpolitik.org 05.01.2012).

Schweiz

Stadt Basel hat ein neues Informations- und Datenschutzgesetz

Am 01.01.2012 ist im schweizer Kanton Basel-Stadt ein neues Gesetz über die Information und den Datenschutz (Informations- und Datenschutzgesetz - IDG) in Kraft getreten. Mit dem Gesetz wird zugleich erstmals in der Stadt Basel ein „Anspruch auf Zugang zu den bei einem öffentlichen Organ ... vorhandenen Informationen“ (§ 25 Abs. 1 IDG) eröffnet. Dieses Gesetz verwirklicht eine vor Jahren auch in Deutschland verfolgte Idee: die Vereinigung des Informationszugangs- und des Datenschutzrechtes in einem Gesetz. Dabei werden die Zugangs- und die Datenschutzregelungen nicht einfach hintereinander gestellt, sondern miteinander verbunden: Nach allgemeinen Bestimmungen (Gegenstand, Zweck, Geltungsbereich, Begriffe) werden „allgemeine Grundsätze für den Umgang mit Informationen“ festgelegt (u. a. Transparenzprinzip, Verantwortung, Auftragsdatenverarbeitung, Informationssicherheit). Ab § 9 IDG sind dann die „Grundsätze für den Umgang mit Personendaten“ festgelegt, ab § 20 die „Bekanntgabe von Informationen“, wobei der generellen Informationsaufgabe von öffentlichen Stellen die datenschutzrechtlichen Übermittlungsregelungen und dann die Veröffentlichung des Verfahrensverzeichnisses folgen. Unter Informationszugangsrechte sind der jeder Person zustehende Zugang zu Verwaltungsdaten normiert, der Auskunftsanspruch zu den eigenen Personendaten sowie die datenschutzrechtlichen Korrekturansprüche. Die „kantonale Aufsichtsstelle“ wird vom „Datenschutzbeauftragten“ geleitet bzw. unter diesem Namen betrieben (§§ 37 ff. IDG).

Damit wird in der Schweiz ein anderer Weg gegangen als in Europa, wo kürzlich mit dem Entwurf einer Datenschutzgrundverordnung die Trennung des Datenschutz- und des Informationszugangsrechts zementiert wird. Die Kombination der beiden Bereiche ist kein basler Unikat, sondern wurde zuvor schon in Solothurn, Zürich, Aargau, Schwyz und im Wallis realisiert. Interessant ist für unser bisher begrenztes Verständnis, das mehr oder weniger im „Recht auf informationelle Selbstbestimmung“ fokusiert, der in § 1 Abs. 2 normierte Gesetzeszwecke: „... das Handeln der öffentlichen Organe transparent zu gestalten und damit die freie Meinungsbildung und die Wahrnehmung der demokratischen Rechte zu fördern, soweit nicht überwiegende öffentliche oder private Interessen entgegenstehen und die Grundrechte von Personen zu schützen, über welche die öffentlichen Organe Personendaten verarbeiten.“ Damit wird sowohl die gesellschaftliche Funktion der Regelungen wie auch ein umfassender digitaler Grundrechtsschutz zum Gesetzeszweck erklärt. Äußerst empfehlenswert und verständlich sind auch die gewählten Formulierungen, die sich ohne Redundanzen und Wiederholungen auf das Wesentliche beschränken und leicht verständlich sind, ohne dabei beliebig oder unklar zu sein und ohne das Schutzniveau abzusenken. Soweit zu einzelnen Regelungen weiterer Präzisierungsbedarf besteht, wurde der durch den Regierungsrat des Kantons in einer „Verordnung über die Information und den Datenschutz“ (Informations- und Datenschutzverordnung - IDV) festgelegt, die auch am 01.01.2012 in Kraft trat.

Auf einer Tagung „Öffentliche Informationen und offene Daten“ am 20.01.2012 beschrieb der Datenschutzbeauftragte des Kantons Basel-Stadt Beat Rudin den Weg dieses Gesetzes: Ein Datenschutzgesetz gab es im Kanton seit 1993. 2006 wurde das Öffentlichkeitsprinzip in der Verfassung des Kantons verankert. Dass es dann doch noch über 5 Jahre dauerte, dass das Prinzip zum Gesetz wurde, ist einer intensiven Diskussion zuzuschreiben. Eine aktive Veröffentlichungspflicht bezieht sich bisher ausschließlich auf Regierungsratsbeschlüsse. Die Beiträge auf der Tagung zeigten, dass der Anspruch auf Informationszugang zu Verwaltungsdaten bisher nur sehr zurückhaltend in Anspruch genommen wird. Eine Erklärung hierfür war, dass in der Schweiz durch die Instrumente der direkten Demokratie ohnehin eine starke Partizipation erfolgt und ein starkes Vertrauen in die Verwaltung besteht. Es bestand aber Einigkeit, dass der Informationsanspruch die demokratische Partizipation und das Vertrauen in die Verwaltung stärkt und nicht behindert. Es wurde zudem klar, dass das IDG nur ein Zwischenschritt ist; Einigkeit bestand, dass das Ziel und der politische Auftrag sei, ein „Open Government Data“ zu realisieren, also eine umfassende aktive Informationspolitik der öffentlichen Verwaltung (Thilo Weichert).

Israel

Saudische Hacker veröffentlichen Daten israelischer Kreditkarten

Eine saudische Hacker-Gruppe „group-xp“ bekannte sich zur Veröffentlichung von Namen, Adressen, Telefonnummern und Karten-Details Tausender Israelis im Internet. Die israelische Zentralbank bestätigte, dass es sich um etwa 15.000 Karten drei verschiedener Firmen handele. Die Unternehmen hätten die betroffenen Kreditkarten bereits identifi-

ziert und blockiert. Die Karteninhaber sollten für den Betrug nicht haften. Der Kartendienstleister Isracard betonte in einer Mitteilung, dass die meisten der entwendeten Daten entweder falsch oder ungültig seien. Der Hackerangriff löste in Israel eine Sicherheitsdebatte aus; die Regierung verglich die Aktion mit einem Terrorangriff. Die Veröffentlichung erfolgte am 02.01.2012 auf der israelischen Sport-Netzseite One.co.il. Über einen Link konnten die Informationen auf Pastebay.com gelesen werden. Erst im November zuvor war es in Israel zu einer schweren Computerpanne gekommen. Die Websites mehrerer Regierungs- und Sicherheitsorganisationen waren nach einem Totalabsturz stundenlang lahmgelegt. Die internationale Hacker-Organisation Anonymous hatte der israelischen Regierung zuvor mit einem Angriff gedroht. Die israelischen Behörden dementierten jedoch damals Berichte über eine Hacker-Attacke und erklärten den Vorfall mit einem technischen Fehler (www.zeit.de 03.01.2012; www.heise.de 04.01.2012).

USA

Neue Gesetze zur Internetkontrolle

Ein Gesetzentwurf im US-Parlament sieht vor, dass Firmen profitieren sollen, wenn sie Nutzerdaten an Behörden liefern. Sie bekämen Geheimdienst-Informationen zu Cyberattacken. Zwar hat der Entwurf zum Stop Online Piracy Act, kurz SOPA, nach heftigem Protest aus der Industrie und der Bevölkerung wenig Chancen, ohne größere Änderungen durch den Kongress zu kommen. Ein anderer Gesetzentwurf, für das freie Internet genauso bedrohlich, könnte dagegen die parlamentarischen Hürden schaffen.

Der Entwurf heißt Cyber Intelligence Sharing and Protection Act. Das Gesetz soll den Austausch von Informationen zwischen Regierungsbehörden wie dem FBI und Computerfirmen wie Microsoft erleichtern, um US-Unternehmen besser vor Cyber-Spionen zu schützen. Nach Einschätzung von BürgerrechtlerInnen wie der American Civil Liberties Union (ACLU) würde es zugleich die bisherigen Bestimmungen zum Schutz der Privatsphäre weitgehend aushebeln. Wegen der ungenauen Formulierungen ist unklar, was unter „Information" oder unter „Cyber-Sicherheit" zu verstehen ist. Die im Gesetzestext enthaltenen Definitionen sind so weit gefasst, dass nahezu alles darunter fällt. Nach Einschätzung des Center for Democracy & Technology (CDT) dürften Firmen wie Facebook, Twitter oder Google dann ohne jede richterliche Anordnung die Anmelde-Daten ihrer NutzerInnen an das FBI, die CIA oder die US-Armee weitergeben. Schließlich diene die Anmeldung am jeweiligen Konto ja dem Schutz des Systems.

Da Netzbetreiber routinemäßig den gesamten Datenverkehr auf mögliche Bedrohungen und versteckte Angriffe hin scannen würden, dürften sie laut dem CDT den kompletten Datenverkehr weiterreichen. Unternehmen wie AT&T, Verizon oder T-Mobile dürften nicht nur mitteilen, wer wann unter welcher IP-Adresse online war, sie dürften auch den Inhalt der über ihre Netze verschickten Nachrichten ohne richterliche Anordnung an die Regierung weitergeben, sofern sie diesen einsehen können. Firmen dürften die Daten sogar untereinander austauschen. Die NutzerInnen hätten dagegen keinerlei Handhabe. Denn mit dem Gesetz würde die US-Regierung den Firmen im Tausch für die Daten Immunität garantieren, also einen Schutz vor Klagen.

Die einzige Hoffnung für VerbraucherInnen ist, dass die Firmen die Daten nicht weitergeben müssen, sondern nur dürfen. Doch auch dafür haben die beiden Abgeordneten, die das Gesetz vorgelegt haben, eine Lösung: Behörden können mit dem Gesetz Firmen belohnen, die bereitwillig Daten tauschen. Als Bonus winkt die Registrierung als Cyber-Security-Firma. An diese Unternehmen dürfen die Regierungsbehörden dann Geheimdiensterkenntnisse aus dem Cyberwar weitergeben. Microsoft könnte etwa über Schwachstellen im Betriebssystem Windows informiert werden, das Softwarehaus Symantec über neue Viren. Den Unternehmen winken mit der Registrierung also wertvolle Informationen, aus denen sich auch Profit schlagen lässt. Zudem wären die registrierten Firmen vermutlich die ersten Ansprechpartner, wenn es um den Schutz der Computernetzwerke der US-Regierung geht. Die Regierungsbehörden dürften die Daten laut dem Gesetzentwurf nicht nur benutzen, um Cyber-Spione zu verfolgen. Die Daten dürfen auch verwendet werden, wenn die nationale Sicherheit – etwa durch Plattformen wie WikiLeaks – bedroht ist. Zudem dürfen sie auch zur Verfolgung ganz gewöhnlicher Straftaten verwendet werden, wenn der Grund für ihre Weitergabe irgendwie mit der Cyber-Sicherheit zu tun hatte.

Der Gesetzestext wurde Ende November 2011 vorgelegt und vom zuständigen Ausschuss bereits einen Tag später bei nur einer Gegenstimme verabschiedet. Da die Vorlage von einem demokratischen und einem republikanischen Abgeordneten gemeinsam vorgelegt wurde, stehen ihre Chancen nicht schlecht – auch wenn das Weiße Haus bereits angedeutet hat, dass den Beratern des Präsidenten das Gesetz zu weit geht. Ob sich Barack Obama mitten im Wahlkampf mit einem Veto angreifbar machen würde, ist allerdings fraglich. Dafür müsste der Widerstand wesentlich größer sein. Um den zu organisieren, fehlt angesichts des rasanten Tempos der Gesetzgebung und der prominenten Unterstützer wie Microsoft oder AT&T wohl die Zeit.

Unternehmen wie Google oder Twitter, die den Cyber Intelligence Sharing and Protection Act ablehnen müssten, konzentrieren sich auf den Stop Online Piracy Act. Auch dieses Gesetz hat das Potential, das Internet grundlegend zu verändern. Mit ihm würde es möglich, ganze Seiten wie YouTube komplett vom Netz zu nehmen oder Internetseiten außerhalb der USA – wie WikiLeaks – finanziell auszutrocknen. Die Aktionen der Gesetzes-GegnerInnen zeigen erste Erfolge. Kurz bevor sich das Parlament in die Pause zu Thanksgiving verabschiedete, riefen nach einem Aufruf der Blogging-Plattform Tumblr Aktivisten an einem Tag mehr als 87.000 Mal ihre Abgeordneten an, um gegen das Gesetz zu protestieren. Auch unter den Abgeordneten wächst der Widerstand. Sowohl die demokratische Fraktions-Chefin Nancy Pelosi, als auch Tea-Party-Ikone Ron Paul haben angedeutet, dem Stop Online Piracy Act in seiner jetzi-

gen Form nicht zuzustimmen. Mit diesen mächtigen Gegnern dürfte sich das Gesetz also zumindest verzögern (Kraft www.zeit.de 05.12.2011).

USA

Handy-Bewegungsprofile in US-Einkaufszentren

In den USA werden zum Zweck der KundInnenbeobachtung Handydaten ausgewertet. Zwei Einkaufszentren haben damit begonnen, die Bewegungen ihrer KundInnen anhand von Handy-Standortdaten zu erfassen. In den Malls Promenade Temecula im Süden Kaliforniens und Short Pump Town Center in Richmond im Bundesstaat Virginia sind seit dem 25.11.2011 Scanner installiert, die die Gerätekennung von Mobiltelefonen registrieren und speichern. Beide Malls gehören zu Forest City, einem amerikanischen Immobilienunternehmen. Das erklärte, der Einsatz der Scanner sei ein Test, um Kundenbewegungen zu beobachten und „das Einkaufserlebnis zu verbessern“.

Die vom Unternehmen eingesetzte Technologie nennt sich Footpath und stammt von einer britischen Firma namens Path Intelligence. Forest City versichert, dass Datenschutz und Anonymität bei dem Verfahren gewahrt blieben. Weder Forest City noch Path Intelligence teilen jedoch mit, welche Daten der Kundenhandys sie genau speichern: „Die Geräte registrieren Signale der Mobiltelefone der Kunden und versenden diese Daten, damit sie ausgewertet werden können. Die Technik sammelt keine persönlichen Informationen oder Telefonnummern.“ Die Scanner registrieren wahrscheinlich die Identifizierungsnummer der SIM-Karte, die sogenannte IMSI. Dafür spricht, dass Path Intelligence die Nationalität der Kunden kennt und diese Information ebenfalls als Auswertungsmerkmal anbietet. Denn die IMSI soll Mobilfunkkunden eindeutig identifizierbar machen – weltweit. Sie enthält dazu unter anderem eine Länderkennung, der Code 262 steht beispielsweise für Deutschland. Jede Nummer wird auch nur einmal vergeben und lässt sich theoretisch zu einem Mobilfunkvertrag zurückverfolgen.

Beide Unternehmen versichern, sie seien an der Identität der Menschen nicht interessiert. Trotzdem sind solche Datenbanken ein Risiko und interessant für Hacker, Kriminelle und Strafermittler. Problemlos lassen sich Gesichter mit den jeweiligen Handystandorten verknüpfen. In solchen Shoppingcentern ist Videoüberwachung allgegenwärtig. Unabhängig davon verraten die Daten viel über das Verhalten der KundInnen: Welche Geschäfte sind beliebt, welche Orte werden so oft frequentiert, dass Werbung dort besonders sinnvoll ist, welche Ecken werden nur kurz angesteuert, in welcher Kombination werden verschiedene Läden besucht, zu welcher Uhrzeit? Problemlos lassen sich so Profile erstellen. Interessante Anwendungen sind denkbar, da die Computer wahrscheinlich jede KundIn nach wenigen Minuten Beobachtung einem bestimmten Profil zuordnen können. Path Intelligence wirbt damit, dass der „Besuchertyp“ identifiziert werden könne, ob also jemand ein „Einkäufer“, ein „Angestellter“, „Hindurchläufer“ oder ein „Muse-Suchender“ sei.

Diese Profile können für gezieltes Marketing genutzt werden, etwa indem den Menschen entsprechende Botschaften auf ihre Handys geschickt werden. Mit der Technik ist auch eine Beeinflussung des Kaufverhaltens vorstellbar. Jene beispielsweise, die als schlechte KundInnen identifiziert werden, bekämen dann eben keine Sonderangebote präsentiert und nicht die Chance, irgendwo einen Rabatt zu erhalten. Die Scanner registrieren auch, ob Handybesitzende wiederkommen. Der Anbieter wirbt auf seiner Website damit, dass unter anderem die „frequency of visits“ gemessen werden könne, die Häufigkeit also, in der eine KundIn die Geschäfte besucht.

Schon das ohne Anlass vollständige Erfassen der IMSI in einem Gebiet ist nach deutschem Datenschutzrecht ein Grundrechtseingriff. Die Speicherung über einen unbekannten Zeitraum zu einem letztlich unbekannten künftigen Zweck macht das Problem noch schlimmer. Auch in den USA regt sich leiser Widerstand. Das Wirtschaftsmagazin Forbes kommentierte, das Ganze „rieche irgendwie illegal“. Die USA sind übrigens nicht der Vorreiter bei einer neuen Überwachungstechnologie. CNN berichtete, die Scanner der britischen Firma seien bereits in Einkaufszentren in Europa und Australien eingesetzt worden. Den KundInnen bleibt die Hoffnung, dass sie das kleine Hinweisschild am Eingang bemerken und ihr Handy rechtzeitig ausschalten. Auch in Europa finden schon heute tendenziell vergleichbare KundInnenanalysen statt: In IKEA-Filialen folgen MitarbeiterInnen ausgewählten KundInnen und beobachten, wohin diese laufen und was sie sich anschauen. In Supermärkten testen Psychologen, welche Regalhöhen, Gangbreiten und Laufwege sinnvoll sind, um so viel wie möglich zu verkaufen. Geschäfte setzen Kameras ein, um Kunden beim Einkaufen auszuspähen. Auf Internetseiten ist weit verbreitet, dass Besuchende mit sogenannten Cookies verfolgt werden um festzustellen, was die Menschen anschauen (Biermann www.zeit.de 28.11.2011).

USA

Polizei von Los Angeles darf nicht in die Google Cloud

September 2010 hatte Randi Levin, Chief Technology Officer und General Manager der Los Angeles Information und Technology Agency noch angekündigt: „Die Stadt Los Angeles wechselt als eine der ersten Verwaltungen in die Cloud. Wir freuen uns über den erfolgreichen Abschluss und widmen uns nun dem finalen Übergang der fünf Dienststellen des Los Angeles Police Departments (LAPD).“ Dave Girourd, President of Enterprise, Google ergänzte: „Google Apps ist die erste komplette Reihe von Cloud-Computing-Anwendungen mit der U.S. Government Security Certification. Los Angeles Mitarbeiter im Bereich öffentliche Sicherheit können zuversichtlich in die Cloud wechseln, da sie die größtmögliche Sicherheit erhalten.“ Doch dazu kommt es nun aus Sicherheitsgründen nicht. Der Stadtrat hat den endgültigen Ausstieg für die Polizei beschlossen, da nach Medienberichten „die Regeln des

Criminal Justice Information System (CJIS) zurzeit nicht mit dem Cloud Computing vereinbar sind und E-Mail-Anwender der Strafverfolgungsbehörden nicht migriert werden können“ (Viola www.egovernment-computing.de 10.01.2012).

USA

„Identified“ – Menschenscoring und -rating für die Arbeitsplatzsuche

Am 19.09.2011 wurde in den USA eine neue Berufssuchmaschine mit dem Namen „Identified“ als Betaversion veröffentlicht, die Menschen mit Scorewerten zwischen 0 und 100 bewertet, um Bewerbenden und Arbeitgebern die Arbeitssuche zu erleichtern. Identified ist das Kind von Brendan Wallace und Adeyemi Ajao, zwei früheren Graduierten der Stanford Graduate School of Business. Wallace hatte danach bei Goldman Sachs und bei der Blackstone Group gearbeitet. Ajao hatte Tuenti.com gegründet, das spanische „Facebook“, das im Juli 2010 von Telefonica für 100 Mio. Dollar erworben wurde. Die Idee für Identified entstand im Frühjahr 2010 aus der Frage: Welche Wirtschaftsausbildung ist besser, um einen Job zu bekommen, die von Stanford oder die von Harvard? Wallace und Ajao meinten, dass sein soziale Netzwerk das wichtigste für eine KandidatIn ist, ein Unternehmen für sich zu interessieren. Sie sammelten für ihre Firma 5,5 Mio. Dollar Gründungskapitel von Investoren, darunter von Googles früherem CEO Eric Schmidt sowie anderen IT-Unternehmern und Wissenschaftlern wie Bill und Tim Draper, Alexander Tamas, Chamath Palihapitiya (Facebook), Joel Peterson und John Glynn (Stanford University). Nachdem Identified im Frühjahr 2011 als Test begann, wurden 80% der Wirtschaftsstudierenden innerhalb von zwei Wochen dort Mitglied. Die Seite hatte damit aus dem Stand mehr Bewerbungsprofile verfügbar als das Stanford Karriere-Förderzentrum.

Die zentrale Funktion von Identified ist die Vergabe von Scores an Personen in drei Bereichen: Berufsleben, Ausbildung und Soziale Netzwerke. Diese Informationen werden vorrangig aus den Profilen von Facebook generiert, weshalb die Menschen ermuntert werden, dort über sich mehr Informationen einzustellen. Wallace und Ajao nennen ihr Verfahren auch „Google-Ranking für Menschen“. Je nach Suche werden die Betroffenen mit 0 bis 100 Punkten bewertet. Eine Person kann im Bereich „Beratung“ hoch und im Bereich „Technik“ niedrig eingestuft sein. Die Seite ging mit mehr als 40 Millionen Personen, wovon die meisten nicht auf der Seite registriert waren, 60.000 Unternehmen und 8.000 Hochschulen an den Start.

Zweck des Ranking und Scoring ist es, Unternehmen die geeignetsten KandidatInnen bei der Jobsuche anzuzeigen. Identified kann auch von Arbeitssuchenden genutzt werden, um sich die bestbewerteten Unternehmen anzeigen zu lassen. Unternehmer und Arbeitsvermittler können z. B. nach TechnikerInnen suchen und erhalten eine Rangliste angezeigt, was vorteilhafter sein soll als die bisher nicht bewertete Liste von LinkedIn. Das Unternehmen verlangt von den nutzenden Unternehmen zunächst einen geringfügigen, potenziell teureren Beitrag. Die Betroffenen können ihren Score im Vergleich zu denen ihrer „Freunde“ oder zu der Gruppe aller Erfassten, ihrer Schule oder ihres Unternehmens sehen. Angezeigt wird auch ein Aktivitätsmaß, etwa, dass das Unternehmen „Disney KandidatInnen zwischen 60 und 80 Punkten“ suchte.

Identified greift die Idee einer neuen Funktionalität von LinkedIn auf, die soziale Kontakte für Leute bei der Jobsuche nutzbar machen will. Es soll aber dabei nicht darauf ankommen, dass die Betroffenen bei dem Dienst selbst aktiv sind. Weiterhin besteht mit Branchout ein weiteres schnell wachsendes Jobvermittlungs-Start-up-Netzwerk, das auf Facebook-Daten beruht. Nach Überzeugung von Wallace liefert aber Identified die besseren Rankings: „Das Problem ist, dass LinkedIn viele Daten auswirft. Wir dagegen sind eine wirkliche Suchmaschine, die berufliche Informationen auf professionelle Weise liefert. Die besten Ergebnisse stehen oben.“

Identified zeigt den Score einer Person sichtbar auf der Seite. In der Testphase konnten die Menschen ihren Score nicht sehen und wussten zumeist gar nicht, dass ein solcher berechnet wird. Es wird sich zeigen, ob sich Personen gegen ihre Scores, vor allem niedrige, zur Wehr setzen werden. Wallace behauptet, dass die Zahl der bei Identified eingehenden Informationen zu einem Ansteigen des Scores führt: „Wir wollen den Nutzenden die Möglichkeit geben, ihre Scores zu organisieren und zu kontrollieren. Ich behaupte nicht, dass eine Person die beste wäre. Es gibt zwar einen übergreifenden Score, aber auch unterschiedliche Scores für unterschiedliche Kategorien.“

Identified wertet auch Freundes-Informationen aus und berechnet Scores von nicht bei Identified registrierten Menschen. Die 40 Millionen Profile zum Start des Angebots stammen weitgehend von den Facebook-Seiten der Betroffenen. Die Profile von registrierten Nutzenden werden veröffentlicht und als Suchergebnisse angezeigt, während Profile von Nichtregistrierten nur von registrierten Identified-Nutzenden eingesehen werden können. Damit will das Unternehmen Menschen ermutigen, Mitglied zu werden. Die Mitglieder finden die Scores und Profile aller 40 Milllionen Menschen sowie von Unternehmen und Universitäten; Nichtmitglieder sehen nur die Mitgliederprofile sowie Unternehmen und Universitäten.

Nach Angaben von Wallace entwickelt Identified seine Kriterien regelmäßig weiter, um die Angaben zum Hintergrund von Leuten, zu Berufstätigkeiten und zur Ausbildung differenziert in die Scores einfließen zu lassen. Mit den Scores aus den Aktivitäten bei Social Communities soll es möglich sein, die Ausbildung auf einer unbekannten Schule zu kompensieren. Wallace behauptet, dass hunderte von Unternehmen die Seite erprobt haben und mit den Ergebnissen zufrieden waren. Die Scores seien keine Beurteilung von Menschen, sondern lediglich die relevantesten Ergebnisse für eine Suche: „Menschen und Unternehmen entscheiden auf der Basis von Priorisierungen. Deshalb lieben sie unsere Rankings.“

Unklar ist, wie die Aktivitäten in Social Communities von Identified bewertet werden. Wichtig ist nach Ansicht von Wallace und Ajao, ob ein Kandidat jemanden in dem Unternehmen oder

das Unternehmen schon kennt oder sich hierfür - zum Beispiel wegen Freunden - dafür interessiert. Ein anderer Indikator sei, das jemand in einem bestimmten Bereich engagiert ist, weil er Freunde aus diesem Bereich hat. Gemäß Ajao kommt es nicht auf die Zahl der Verbindungen bei Facebook an, sondern darauf, wie die Beziehungen zu den besser bewerteten KandidatInnen sind. Dazu kann gehören, ob sie die gleiche Schule besuchten, gemeinsam in einer Firma oder in einem Team arbeiteten, gegenseitig auf ihren Seiten Kommentare einstellten und Ähnliches.

Harvard wird höher eingestuft als Stanford, weil bei einer Bewertung die Unternehmen aller AbsolventInnen von Harvard besser abschneiden als die mit Studierenden aus Stanford. Auf der Seite können BesucherInnen nachschauen, welche Freunde von ihnen in einem Unternehmen arbeiten, von welchen Schulen die Beschäftigten des Unternehmens kommen, wo sie vorher und nachher beschäftigt waren und wie es im Vergleich zu anderen Unternehmen steht. Hunderte Unternehmen nutzen inzwischen die Seite, z. B. Barclays, McKinsey, Google, Disney, Sequioa Capital, Levi Strauss und MTW. Wallace und Ajao erwarten, dass ihre Seite schnell weiterwachsen wird. Ihr Dienst sei nicht nur für die Jobsuche nützlich, sondern auch für andere wirtschaftliche Zwecke (Geron www.forbes.com 19.09.2011: „Identified launches its People-Ranking“; Weichert News www.datenschutz.de 20.12.2011).

USA

Staatsanwältin zwingt zu mehr Transparenz bei Smartphones

Kaliforniens Generalstaatsanwaltschaft hat Apple, Google, Microsoft, den Blackberry-Anbieter RIM, Amazon und Hewlett-Packard zu mehr Transparenz bei Apps für Smartphones verpflichtet. Rund 600.000 Apps vertreibt Apple derzeit für seine iPhone- und iPad-KundInnen, etwa 400.000 bietet der Konkurrent Google für Androidgeräte an - ein riesiger Markt, der stetig wächst. Und ein massives Problem für den Datenschutz. Am 22.02.2012 verkündete Kaliforniens Generalstaatsanwältin Kamala Harris den Abschluss einer Vereinbarung, wonach künftig jede App, die die sechs Internetkonzerne anbieten, bestimmte Datenschutz-Standards erfüllen muss. So sollen die NutzerInnen darüber informiert werden, welche Daten mit dem Download von ihnen gesammelt und wozu sie verwendet werden. Das geschehe bisher nur in den seltensten Fällen, monierte Harris. Außerdem soll festgeschrieben werden, an welcher Stelle die Nutzer die jeweiligen Datenschutzbestimmungen des Anbieters finden.

Apps sind Anwendungen für Smartphones. Um mit ihrer Hilfe zum Beispiel mit Freunden zu chatten, benötigen Apps Zugriff auf private Daten. Das muss normalerweise zuvor erlaubt werden. Das Auslesen von Adressdaten ist auf dem iPhone wie auch auf Android-Smartphones möglich. Anders als bei Apple erfordert Googles Betriebssystem die Zustimmung des Nutzers. Gefährlich ist das heimliche Auslesen der Daten. Dubiose App-Entwickler bieten vermeintlich attraktive Anwendungen kostenlos und verkaufen nach der Installation die ausgespähten Daten. Harris will binnen sechs Monaten sicherstellen, dass sich die NutzerInnen auf den Plattformen der Giganten über die Datenschutz-Bedingungen der einzelnen Anwendungsprogramme informieren und Apps, die gegen die Richtlinien verstoßen, melden können. Die Firmen wiederum verpflichten sich, solche Meldungen umzusetzen und die Entwickler der Programme zu kontrollieren.

Der Datenschutzbeauftragte von Schleswig-Holstein, Thilo Weichert, zeigt sich von der US-amerikanischen Einigung wenig beeindruckt: „Die Vereinbarung ist ein erster richtiger Schritt, aber sie bleibt weit hinter dem zurück, was aus europarechtlicher Sicht selbstverständlich sein sollte.“ Es sei „unbefriedigend“, dass die USA als Sitz der großen Internetkonzerne solch „unzureichende“ Datenschutz-Standards setzten - auch weil „die Bundesregierung sich als absolut unfähig erweist“, hier etwas zu tun. Nach europäischem Recht seien die Anbieter von Anwendungsprogrammen nicht nur zur Information verpflichtet. Sie müssten den Nutzenden eine Wahl lassen. Diese müssten die Möglichkeit haben, eine App zu nutzen, ohne andere Daten als die für den Dienst notwendigen preiszugeben: „Der Datenmissbrauch über solche Anwendungen ist ein Riesenproblem, das immer mehr überhand nimmt und das wir noch nicht einmal ansatzweise in den Griff bekommen haben.“ Die Aufsichtsbehörden müssten mehr Ressourcen bekommen, um wirksamer auf die Konzerne, etwa über ihre deutschen Dependancen, einwirken zu können. Die europäische Datenschutzgrundverordnung, die im Januar vorgestellt wurde, müsse schnellstens verabschiedet werden, um wirksame Sanktionen gegen Datenmissbrauch zu ermöglichen.

Auch die amerikanische Regierung beginnt Datenschutzverstößen größere Aufmerksamkeit zu widmen. Am 22.02.2012 schlug das Weiße Haus eine „Bill of rights“ vor, einen Katalog von sieben Rechten für Internetnutzende. An erster Stelle steht dabei, diesen mehr Kontrolle darüber zu geben, welche persönlichen Daten von ihnen im Internet gesammelt und wozu sie verwendet werden. Nach Angaben der Regierung haben außerdem mehrere Internetunternehmen zugestimmt, den Nutzenden zu ermöglichen, mit einem einfachen Klick zu verhindern, dass Daten von ihnen eingesammelt werden („do not track“).

Das Geschäft mit den Apps wächst rasant. 35 Milliarden Apps sind bisher auf Mobilgeräte heruntergeladen worden, bis 2015 sollen es Schätzungen zufolge bereits 98 Milliarden sein. Im gleichen Zeitraum soll sich der Umsatz mit den Mobilanwendungen von 6,8 Milliarden Dollar auf 25 Milliarden Dollar vervierfachen. Schon jetzt bieten mehr als 50.000 EntwicklerInnen ihre Programme an, meist über die Plattformen der großen Konzerne. Immer wieder werden Apps für Datenklau missbraucht. Erst kürzlich wurde bekannt, dass die App des Online-Netzwerks Path ohne Wissen der NutzerInnen deren Adressbücher anzapfte und die Daten speicherte. In einem Blogeintrag entschuldigte sich das Unternehmen bei den Nutzenden und bestätigte, dass alle Kontaktdaten

der Nutzenden nun gelöscht seien. Auch die Twitter-App sammelte die Kontaktdaten der Nutzer ein. Zudem häufen sich laut Weichert die Fälle von Betrug mit geklauten Daten. Dabei würden die Kontodaten der Nutzer für illegale Abbuchungen genutzt (Erb www.fr-online.de 23.02.2012; Lindner/Heeg www.faz.net 23.02.2012; Bernau SZ 24.02.2012, 1).

USA

Anonymous hackt Stratfor

AktivistInnen der Hacker-Bewegung Anonymous haben Server des auf globale Sicherheitsanalysen spezialisierten US-Unternehmens Strategic Forecasting (Stratfor) angegriffen und sich dabei eigenen Angaben zufolge Zugriff auf mehr als 200 Gigabyte Daten verschafft. Stratfor-Gründer George Friedman bestätigte, dass eine Liste mit eigentlich vertraulichen „Namen unserer Geschäftskunden auf anderen Webseiten veröffentlicht“ wurde. Sie umfasst rund 4.000 Einträge, als Stratfor-Kunden werden unter anderem die Deutsche Bank, DHL und das Nachrichtenmagazin Der Spiegel genannt.

Schwerwiegender als die Veröffentlichung von Kundennamen ist wohl, dass die Anonymous-AktivistInnen Kreditkarteninformationen von Stratfor-KundInnen abgegriffen haben: Über Twitter verbreiteten sie die Nachricht, tausende Kreditkarten für Zahlungsanweisungen nutzen zu können. Als Beweis veröffentlichten sie Screenshots von Online-Überweisungen. Die AktivistInnen waren über die Weihnachtsfeiertage in die Kundendatei von Stratfor Global Intelligence Service eingedrungen. Die Firma rühmt sich, ihren KundInnen mit angeblich exklusiven Analysen mehr Sicherheit bieten zu können. Bis zu 90.000 Namen, Adressen und Kreditkarten-Infos will Anonymous für Umverteilungen à la Robin Hood genutzt haben. Befragte Betroffene bestätigten gegenüber US-Medien, dass es zu nicht autorisierten Zahlungsanweisungen gekommen sei. Anonymous erklärte, auf diesem Weg mehr als eine Million Dollar an Hilfsorganisationen und „Bedürftige in den ganzen USA“ verteilen zu wollen. Ein Mitarbeiter von Amerikas mächtigem Heimatschutzministerium überwies so unfreiwillig 180 Dollar an das Rote Kreuz; ein früherer Angestellter der Bankenaufsicht in Texas entrichtete unwissentlich 200 Dollar für denselben guten Zweck. Es sei, so rechtfertigten die Aktivisten des Hacker-Netzwerkes ‚Anonymous‘ ihren Raubzug, schließlich Weihnachten.

Die Liste der Stratfor-KundInnen ist eindrucksvoll: Das Verteidigungsministerium, der Rüstungskonzern Lockheed Martin und das berühmte Atomforschungslabor in Los Alamos finden sich ebenso unter den Opfern wie Microsoft und Apple oder zahllose einfache US-BürgerInnen. Anonymous ergoss Spott über Stratfor und erklärte, der Angriff sei deshalb so leichtgefallen, weil die Firma die Daten ihrer Kunden nicht einmal verschlüsselt habe. Am zweiten Weihnachtsfeiertag prangte auf der Homepage der Firma eine vertröstende Nachricht: „Diese Seite wird derzeit gewartet. Bitte besuchen Sie uns bald wieder.“ Fred Burton, im Strafor-Vorstand unter anderem für geheimdienstliche Fragen zuständig, sagte, die Hacker lebten offenbar „in einer Welt, in der es außergewöhnlich schwer ist, sich gegen Angriffe zu verteidigen, wenn sie sich erst einmal auf dich eingeschossen haben“.

In einer öffentlichen Stellungnahme erklärte Anonymous, nicht sie als bekannte Hacker-Organisation, sondern „aufmerksamkeitsgeile Opportunisten“ seien verantwortlich, was offenbar eine Anspielung auf die „Lulzsec“-Gruppe war, die in der Vergangenheit gestohlene E-Mail-Passwörter veröffentlicht hatte. Dem Dementi folgte allerdings wieder ein Dementi, das wie alle Mitteilungen über die anonyme Online-Publikationsplattform Pastebin veröffentlicht wurde: Natürlich stekke Anonymous hinter der Aktion. In einer derart losen wie führungslosen Vereinigung könne niemand bestimmen, ob eine Operation dem Kollektiv zuzuschreiben sei oder nicht. Anonymous hatte wiederholt mit spektakulären Aktionen Aufsehen erregt: Erst kurz zuvor hatte man die Homepage des syrischen Verteidigungsministeriums lahmgelegt, um gegen die blutige Niederschlagung der Demokratiebewegung zu protestieren. Im November 2011 suchte Anonymous das Duell mit dem mexikanischen Drogenkartell und drohte, man werde die Namen zahlloser Mafiosi veröffentlichen, falls ein entführter Internet-Rebell nicht sofort freigelassen würde. Angeblich obsiegte Anonymus. Und vor einem Jahr hatten die Hacker, deren Markenzeichen die Maske des legendären englischen Brandstifters Guy Fawkes ist, Großbanken und Kreditkarten-Konzerne angegriffen. Zuvor hatten sich diese geweigert, Spenden für das Enthüllungsportal Wikileaks zu transferieren. Die Weihnachtsaktion erinnerte auch an Bradley Manning: Der wegen Geheimnisverrats inhaftierte US-Soldat, der mutmaßlich Regierungsdokumente an Wikileaks gegeben hatte, solle statt Strafe besser „ein anständiges Essen“ bekommen, so Anonymous. Das Netzwerk kündigte weitere Aktionen an.

Der Gruppe gemeinsam ist, den vermeintlich Mächtigen Grenzen aufzuzeigen, wenn deren Handlungen den Vorstellungen der Mitglieder nicht entsprechen. US-Kommunikationswissenschaftlerin Gabriella Coleman, die über die Gruppe seit Jahren forscht, erläuterte: „Die Mitglieder sind unglaublich verschieden.“ Einige europäische Mitglieder seien „beinahe adelig“, andere „unterhalb der Arbeiterklasse“. So unterschiedlich der persönliche Hintergrund ist, so verschieden sind offenbar auch die Meinungen, wer zu den zu entlarvenden Mächtigen gehört. Zu der neuesten Aktion meinte Virenexperte Mikko Hyppönen, die bedachten Wohltätigkeitsorganisationen würden im Ergebnis nicht profitieren, sondern hätten eher Ärger: „Diese Gelder werden niemals diejenigen erreichen, die sie brauchen.“ Vielmehr müssten die Spendenempfänger die fälschlich erhaltenen Summen zurückbuchen, sobald die Kreditkartenfirmen diese als illegal klassifizieren, und damit Geld und Arbeitszeit aufwenden (www.heise.de 26.11.2011; Wernicke SZ 27.12.2011, 6; Kuhn SZ 28.12.2011, 4, 19).

USA

„Carrier IQ"-Software sammelt Daten in über 140 Millionen Handys

Das Programm Carrier IQ (CIQ) steckt in vielen Smartphones in den USA und zeichnet das Nutzerverhalten auf – auch Texteingaben, die eigentlich verschlüsselt werden sollen. Auf der Website des Unternehmens Carrier IQ läuft ein Zähler, der Ende 2011 mehr als 141 Millionen anzeigte, Tendenz steigend, womit angezeigt wird, wie viele Smartphones derzeit im Umlauf sind, die eine Software installiert haben, die wie das Unternehmen heißt. Aber nur die wenigsten der Handybesitzenden wissen, dass CIQ auf ihren Geräten versteckt ist, und was die Software alles kann.

Der 25jährige Android-Entwickler Trevor Eckhart beschreibt in einem Video, wie er diese Software auf seinem HTC-Smartphone gefunden hat, und dass sie sich nicht stoppen lässt. Der einzige Weg sie loszuwerden, ist ihm zufolge das Betriebssystem auszutauschen. Die Funktionen der Software sind umfassend: CIQ kann Standortinformationen, eingehende Anrufe und SMS ebenso aufzeichnen wie das Aufrufen von Apps. Sie kann Audioaufnahmen starten – und sogar Eingaben auf der physischen und der virtuellen Tastatur des Geräts protokollieren. Auf den meisten in den USA verkauften Android-Geräte, Blackberrys und Nokia-Smartphones ist, so Wired.com, CIQ installiert. Die Nutzenden erfahren davon nichts. Allenfalls bei bestimmten Systemabstürzen fragt das Gerät, ob es eine entsprechende Fehlermeldung an den Hersteller oder den Provider senden darf. Das Programm diene dazu, Providern Infos über Handyempfand und Gespräche zu liefern, um auf dieser Basis ihre Services verbessern zu können. Dafür, so Carrier IQ, werde die Software gebraucht. Sie soll helfen, die Qualität und Stabilität von Netzwerken und Hardware zu verbessern, indem sie Informationen über Abstürze und andere Fehlfunktionen sammelt. Tastatureingaben würden nicht aufgezeichnet. HTC und der Mobilfunkanbieter Sprint gaben ähnliche Erklärungen ab.

Eckhart zeigt in seinem Video, wie er auf seinem HTC Evo die Worte Hello World in die HTTPS-Suche von Google eingibt. Im Protokoll, das CIQ anlegt, erscheinen diese Worte im Klartext. Das bedeutet, dass die Software Texteingaben sehr wohl aufzeichnet. Sie ist dabei sogar in der Lage, das HTTPS-Protokoll zu unterlaufen, indem sie jeden Buchstaben schon beim Eintippen speichert. HTTPS verschlüsselt erst beim Absenden des Textes. Eckhart konnte sich, so seine Angaben, auch eine Fabrikversion der Software ansehen. In ihr sei vorgesehen, dass Nutzende bei Abstürzen eine Liste zu sehen bekommen, auf der sie ihre technischen Probleme benennen können. CIQ mache sich dabei mit einem Symbol in der Statusleiste bemerkbar. Auf verkauften Geräten aber sei das nicht selbstverständlich – die Software könne modifiziert und komplett verborgen werden. Eckhart bezeichnet CIQ deshalb als Rootkit, also als ein Werkzeug, mit dem sich jemand heimlich Administratorrechte für ein Gerät sichert. Nicht nachgewiesen wurde, dass Daten, wie etwa die Texteingaben, auch an irgendeinen Server gesendet werden. Deshalb forderte Eckhart vom Unternehmen selbst, von den Geräteproduzenten und den Mobilfunkbetreibern nur, dass sie die Smartphone-Besitzenden besser und transparenter darüber aufklären, dass die Software vorhanden ist, was sie kann und welche Informationen sie tatsächlich sendet.

Nicht jedes Handy läuft mit CIQ-Software. Meist wird das Programm zur Systemdiagnose in „Operator-Smartphones" eingesetzt, also Mobiltelefonen, die Hersteller direkt für Mobilfunkanbieter bauen und entsprechend modifizieren. Ob CIQ auch außerhalb der USA eingesetzt wird, ist unklar. Nokia erklärte, dass bei dessen Smartphones die Software nicht installiert sei.

Anfragen bei dem Unternehmen selbst sowie bei HTC wurden zunächst nicht beantwortet. In einer Stellungnahme hieß es dann, man sammele anonymisiert „operative Informationen". Damit könnten Provider Verbindungsprobleme aufgrund schwacher Netzleistung ausmachen und beheben: „Wir zeichnen nicht auf, welche Tasten gedrückt werden und liefern keine Überwachungswerkzeuge." Um Genaueres herauszufinden, können fortgeschrittene Nutzende eine von Eckhart entwickelte Software nutzen, die Carrier IQ in Android-Geräten aufspüren soll. Eine Unterlassungsklage gegen Eckhart und die Forderung nach 150.000 Dollar Schadenersatz wegen Verleumdung zog Carrier IQ nach einer Intervention der Bürgerrechtsorganisation Electronic Frontier Foundation zurück und entschuldigte sich dafür (Beuth www.zeit.de 30.11.2011; Kuhn www.sueddeutsche.de 30.11.2011).

USA

Mobiler Körperscanner in New York

Die New Yorker Polizei setzt einen mobilen Terahertz-Scanner ein, mit dem künftig versteckte Waffen entdeckt und so schneller aus dem Verkehr gezogen werden sollen. Die Methode soll, so der Plan der Behörde, zur „sicheren Alternative" zur Durchsuchung verdächtiger Personen entwickelt werden. Der neue Scanner soll Verdächtige scannen, während die PolizeibeamtInnen in ihrem Wagen sitzen bleiben. Das als „Drive-by Gun Scan" vorgestellte Verfahren soll bis zu einer Entfernung von 4,5 Metern Gegenstände wie Pistolen oder Messer orten können. Das Gerät misst die Terahertz-Wellen, die von Menschen abgestrahlt werden, und die Textilien, Plastik oder Papier durchdringen. Objekte aus Metall, die als Leiter für diese Wellen undurchlässig sind, zeichnen sich dagegen auf dem Wärmebild des Menschen mehr oder weniger deutlich ab. Die Reichweite des Scanners soll bis auf 23 Meter ausgedehnt werden. Möglich werden soll das durch eine Forschungskooperation zwischen der New Yorker Polizei und dem Pentagon.

Bürgerrechtsgruppen kritisieren, dass bereits jetzt vor allem Farbige und Latinos durchsucht werden: Von den knapp 600 000 Menschen, die 2010 in New York angehalten und abgetastet worden sind, waren gemäß dem Center for Constitutional Rights in New York 87% dieser Herkunft. Eine geheime Durchsuchung

potenziell verdächtiger Personen ohne deren Wissen würde diesen Anteil wahrscheinlich weiter in die Höhe treiben. In Deutschland sind Forschungsarbeiten an einer passiv arbeitenden „Teracam" im Rahmen des Verbundprogramms „Forschung für die zivile Sicherheit" bis 2010 gefördert worden. Resultate zu dem Projekt liegen bislang jedoch nicht vor (www.heise.de 30.01.2012).

Indien

Regierungsabhörschnittstelle bei Apple, RIM und Nokia?

Die Hackergruppe „The Lords of Dharmaraja" veröffentliche Dokumente, aus denen hervorgeht, dass die Smartphone-Hersteller Apple, Nokia und Research in Motion (RIM) einem indischen Geheimdienst Zugang zu den E-Mails ihrer KundInnen gewähren. Der US-amerikanische IT-Sicherheitsexperte Christopher Soghoian wies in einem Tweet auf die Veröffentlichung dieser Hackergruppe hin: „Hacker haben eine interne geheime Mitteilung des indischen Militärgeheimdienstes veröffentlicht, nach denen Apple Abhörhintertüren für die Regierung bereitstellt." Dort heißt es: „Wir veröffentlichen Informationen von Servern des indischen militärischen Geheimdienstes." Ein Dutzend Softwarefirmen hätten die Vereinbarung unterzeichnet. Den Hackern liege der Quellcode der Hintertüren der Firmen vor. Als „Gegenleistung" hätten die mit „RINOA" abgekürzten Unternehmen, was für RIM, Nokia und Apple steht, Zugang zum indischen Markt erhalten. Ob die veröffentlichten Dokumente echt sind, blieb unbestätigt.

Über diese Abhörschnittstelle soll die indische Regierung auch E-Mails der U.S.-China Economic and Security Review Commission mitgelesen haben, die sich mit Sicherheitsfragen der Beziehungen zwischen den USA und China beschäftigt. Als Beweis dafür veröffentlichten die Hacker Teile aus der E-Mail-Korrespondenz des Kongressausschusses. Die indische Regierung hatte RIM im Jahr 2010 ein Ultimatum gestellt, ihren Behörden Zugang zu der E-Mail-Kommunikation über die Blackberrys zu gewähren. Textnachrichten können die Behörden bereits abhören – den Zugang dazu hatte RIM bereits gewährt (DANA 3/2011, 127 f.). Der indische Staat verlangte jedoch auch Zugriff auf die von Blackberry-Nutzenden versandten verschlüsselten E-Mails.

Nokia erklärte, keinen Kommentar abgeben zu wollen. Blackberry-Hersteller RIM dementierte die Meldungen. Die technischen Möglichkeiten zum Abhören verschlüsselter Kommunikation habe man gar nicht. Auch Apple dementierte: Man habe der indischen Regierung keine Zugriff über Hintertüren auf Apple-Software ermöglicht. Die indische Armee, von der die Überwachung ausgehen soll, dementierte ebenso alle Vorwürfe. Die Hacker würden bösartige Absichten verfolgen, das Dokument sei gefälscht. Indien macht jedoch kein Geheimnis daraus, Privat- und Geschäftshandys etwa im Kampf gegen terroristische Separatistengruppen abzuhören. Tatsächlich ist das staatliche Abhören Gesetz und zumindest Blackberry-Hersteller RIM unterstützt die indische Regierung gemäß westlichen Presseberichten beim Lauschangriff.

Dass die Hackergruppe keine reine Luftnummer ist, bewies sie, als Antivirus-Hersteller Symantec vor einigen Tagen einräumte, dass die Gruppe Teile des Quellcodes von zwei älteren Versionen ihrer Antivirus-Produkte entwendet hatte - die Codepassagen seien vier, beziehungsweise fünf Jahre alt. Symantec räumte die Authentizität des Quellcodes ein, konnte aber nicht erklären, woher der Code gekommen war. Die eigenen Systeme jedenfalls seien nicht geknackt worden. Die Hacker drohten mit weiteren Veröffentlichungen: Auf dem von ihnen geknackten Geheimdienst-Server hätten sie Quellcodes von rund einem Dutzend anderer Software-Firmen entdeckt, die alle ein Abkommen mit dem indischen „Tactical Network for Cellular Surveillance (TANCS)"-Programm und dem Central Bureau of Investigation (CBI) unterzeichnet haben sollen, um das weitgehende Abhören von Mobilfunk- und Datenverkehr in Indien zu ermöglichen (Sawall www.zeit.de 10.01.2012; www.spiegel.de 10.01.2012).

Syrien

Überwachungskooperation mit Deutschland beendet

Zwei mutmaßliche syrische Spione wurden am 07.02.2012 in Berlin festgenommen und in Untersuchungshaft gebracht; vier Mitarbeiter der syrischen Botschaft in Berlin wurden ausgewiesen. Die Bundesanwaltschaft ließ außerdem die Wohnungen von sechs Beschuldigten durchsuchen, denen der Vorwurf gemacht wird, seit Jahren Oppositionelle bespitzelt zu haben. Nach Angaben der Bundesanwaltschaft beobachtet der deutsche Verfassungsschutz schon länger die Beschuldigten. Im jüngsten Verfassungsschutzbericht heißt es, syrische Geheimdienste würden in der Botschaft in Berlin eine „Legalresidentur" unterhalten, also einen Stützpunkt eines fremden Nachrichtendienstes - „abgetarnt" in einer offiziellen Vertretung des Gastlandes. Auf diese Weise führe Syrien ein Agentennetz und schrecke bei der Werbung neuer AgentInnen und der Einschüchterung von GegnerInnen nicht vor „Repressalien" zurück. Das Auswärtige Amt schloss nach den Verhaftungen weitere Maßnahmen gegen die syrische Vertretung ausdrücklich nicht aus. Damit gingen Bundesregierung und deutsche Justiz zu dem Geheimdienst des nahöstlichen Diktators Baschar al-Assad auf Distanz. Syrien plante zunächst eine Retourkutsche: In Damaskus wurden Erkundigungen über dort lebende BND-Agenten eingeholt. Die Revanche scheiterte, weil die drei Residenten des deutschen Auslandsgeheimdienstes zusammen mit Botschaftsangehörigen bereits ins libanesische Beirut ausgereist waren.

Die Distanz bestand nicht immer. Nach 2002 arbeiteten die Nachrichtendienste beider Länder vorübergehend eng zusammen. Der konkrete Anlass waren die Anschläge vom 11.09.2001 und der Kampf gegen das Terrornetzwerk al-Qaida. An vielen Knoten dieses Netzwerkes saßen Syrer. Vom syrischen Geheimdienst versprach man sich Unterstützung. Er betrachtete den islamistischen Terror auch als Bedrohung

des Regimes in Damaskus. Die deutschen Sicherheitsbehörden standen unter Druck, weil die Attentäter des 11.09.2001 ihre Taten in Hamburg vorbereitet hatten. Besonderes Interesse hatten die deutschen Ermittelnden an dem in Hamburg lebenden Deutsch-Syrer Mohammed Haydar Zammar, der enge Verbindungen zu den Attentätern unterhalten hatte. Eine Unterstützung oder gar Mittäterschaft konnte ihm jedoch nicht nachgewiesen werden, weshalb Zammar im Dezember 2001 ungehindert nach Marokko reisen durfte. Dort wurde er auf Betreiben der USA verhaftet und nach Syrien gebracht, wo er weiterhin inhaftiert ist. Dass die Deutschen dabei die Hand im Spiel hatten, wurde von einem Untersuchungsausschuss des Bundestags im Jahr 2009 verneint.

Zammar spielte dennoch in den deutsch-syrischen Geheimdienstbeziehungen eine wichtige Rolle. Am 10.07.2002 empfing der damals für die Nachrichtendienste zuständige Abteilungsleiter im Kanzleramt, Ernst Uhrlau, in Berlin den stellvertretenden Leiter des syrischen Militärgeheimdienstes, Assif Schaukat. Der ist ein Schwager Assads und mittlerweile Vize-Verteidigungsminister. Bei dem Treffen im Kanzleramt fragte Uhrlau, der später Präsident des Bundesnachrichtendienstes (BND) wurde, auch nach Zammar. 14 Tage danach wurde, nur wenige Stunden vor seinem Beginn, der Prozess gegen zwei syrische Spione eingestellt, die in Deutschland syrische Oppositionelle drangsaliert hatten. Im November 2002 reisten fünf Beamte des BND, des Bundesamtes für Verfassungsschutz und des Bundeskriminalamtes nach Damaskus und vernahmen drei Tage lang den dort inhaftierten Zammar. Den Verdacht, die Einstellung des Prozesses sei die Gegenleistung für die Erlaubnis zur Befragung Zammars gewesen, erachtete sieben Jahre später der Untersuchungsausschuss für widerlegt. Der Ausschuss meinte, man habe mit der Einstellung des Prozesses das Klima für die Zusammenarbeit bei der Bekämpfung des Terrorismus allgemein verbessern wollen. Zu diesem Zweck war auch schon im Mai 2002 das Bundestagsgremium für die Kontrolle der Geheimdienst (PKG) nach Damaskus gereist. Letztlich wurde aus der erhofften Zusammenarbeit nicht viel. Die syrischen Hinweise auf al-Qaida blieben dürftig. Die Repressalien syrischer Agenten gegen Oppositionelle in Deutschland gingen bis in die jüngste Zeit weiter.

Im Dezember 2011 wurde der syrische Oppositionelle und Grünen-Politiker Ferhad Ahma in seiner Wohnung in Berlin von zwei Unbekannten zusammengeschlagen. Er vermutete dahinter „Schergen des Assad-Regimes“. Er steht auf einer Liste mit 287 Exil-Syrern, die dem Infoportal kurdwatch.org zugespielt wurde, deren Echtheit nicht überprüft werden kann. Die Genannten sollen „wegen Verbrechen gegen den Staat“ gesucht werden und erst Reisedokumente erhalten, wenn sie zuvor syrische Sicherheitsdienste kontaktiert haben. Ahma ist Mitglied des Nationalrats der syrischen Opposition. Deutsche Ermittler stellten seit den Unruhen in Syrien fest, dass die Oppositionsbewegung in Deutschland deutlich intensiver ausgespäht wird. Verschiedene Dienste würden mit eigenen Zuträgern Berichte über Veranstaltungen von regimekritischen ExilsyrerInnen anfertigen und z. B. Portraitfotos in hoher Auflösung von einzelnen DemonstrantInnen in die Heimat schicken. Deutschen Behörden ist es offensichtlich gelungen, teils aus Internetcafés verschickte Spitzelberichte, z. B. an den Militärgeheimdienst, abzufangen. In Deutschland leben mehr als 32.000 syrische StaatsbürgerInnen. Ein Sprecher von „Adopt a Revolution“ meinte, viele hätten Angst, dass Angehörige in ihrer Heimat bedroht und verfolgt würden. Die Leiterin des Berliner Verfassungsschutzes Claudia Schmidt erläuterte am 15.02.2012 im zuständigen Ausschuss des Abgeordnetenhauses, dass Syrer angeworben würden, indem Repressalien gegen Verwandte in der syrischen Heimat angedroht werden (Schultz SZ 08.02.2012, 1, 7; Blechschmidt SZ 11./12.02.2012, 6; SZ 16.02.2012, 5; Der Spiegel 1/2012, 12; Der Spiegel 7/2012, 18; siehe auch DANA 4/2011, 181).

Technik-Nachrichten

Sicherheitslücke bei Amazon-Cloud

Forschende der Ruhr-Universität Bochum haben eine Sicherheitslücke beim Online-Buchhändler Amazon aufgedeckt. Juraj Somorovsky, der am Lehrstuhl für Netz- und Datensicherheit forscht und die Idee zu dem simulierten Hacker-Angriff hatte, erläuterte: „Wir hatten Zugriff auf alle Daten eines Kunden, hätten auch gespeicherte Daten verändern können.“ Bereits Ende 2010 hatte das Forscherteam das Unternehmen über die Sicherheitslücke informiert, das, so Somorovsky, das Leck inzwischen behoben hat. Wegen komplizierter Verfahren beim Veröffentlichen von wissenschaftlichen Arbeiten hat die Universität ihre Forschungsergebnisse jedoch erst einige Monate später preisgegeben. Mit einem selbst geschriebenen Mini-Programm gelang es dem Team vom Lehrstuhl für Netz- und Datensicherheit, den Account einer beliebigen KundIn des von Amazon angebotenen Cloud-Service komplett zu übernehmen und dessen Daten einzusehen und zu bearbeiten. „Das wäre auch mit jedem anderen Account möglich gewesen“. Somorovsky legt Wert darauf, dass keine fremden Daten ausgespäht wurden. Darüber hinaus entdeckten die Forschenden Sicherheitslücken im Online-Shop von Amazon und bei einem weiteren Anbieter. Die sogenannte Cloud bietet KundInnen Online-Speicherplatz. Sie gilt als zukunftsweisende Innovation

und findet immer mehr Verbreitung. Deswegen sei es dringend notwendig, die Sicherheitslücken zu erkennen und zu vermeiden. Die WissenschaftlerInnen nutzten bei ihren Angriffen Schad-Codes oder Mini-Programme, die Daten von NutzerInnen abfangen und weitergeben können (Stürzenhofecker www.welt.de 24.10.2011).

Sensorpflaster zum Aufkleben

Eine Forschergruppe um Dae-Hyeong Kim von der Universität Illinois/USA hat eine Schaltung entwickelt, mit der die medizinische Datenerfassungen über aufklebbare Microchips erfolgen können, die danach wieder einfach und ohne Schmerzen oder Jucken zu beseitigen sind. Gemessen werden können Puls, Hirnströme, Muskelaktivitäten und sogar Sprache. Das Sensorpflaster wurde in einer Ausgabe der Zeitschrift Science vorgestellt (Bd. 333, S. 830, 2011). Auf der Größe einer Briefmarke sind Sensoren und Antennen zusammengefasst zur kabellosen Übertragung und mit einer eigenen Energieversorgung durch die Aufnahme und Umwandlung von Wärme- oder Lichtstrahlung. Einer der Autoren, John Rogers, erläuterte: „Wir wollten ein Gerät erschaffen, das die Anwendenden nicht spüren und das unsichtbar ist“. Das Sensorpflaster könne sich der Haut anpassen und jede Verformung mitmachen. Die Schaltkreise sitzen auf einer extrem dünnen Schicht Kunststoff, die von selbst haftet. Die Leitungen bilden Serpentinen, so dass sie sich verformen können. Sie Sensoren können in ein abwaschbares Tattoo integriert und so getarnt werden. Das Pflaster klebt bis zu 24 Stunden lang und versendet Messdaten durch integrierte Antennen. Je nach dem Ort verschickt es unterschiedliche Daten: Auf der Brust misst es den Herzschlag, am Bein erkennt es, ob die Person geht oder steht. Auf der Stirn aufgeklebt zeigt es an, ob die Augen geöffnet oder geschlossen sind. Das Pflaster kann auch zur Kommunikation zwischen Mensch und Maschine genutzt werden. Auf den Hals einer ProbandIn geklebt, kann diese mit Worten wie „rauf“ und „runter“ ein Videospiel mit einer Genauigkeit von mehr als 90% steuern. Die Feineinstellungen machen aber noch Probleme, da wegen der starken Biegbarkeit der Schaltkreise die gesendeten Signale noch von der Form der Leitungen abhängt, so Rogers: „Unsere Arbeit fängt gerade erst an“ (Behrens SZ 12.08.2011, 16).

Computer lesen Gedanken

Das amerikanische Verteidigungsministerium forscht daran, per Hirnstrommessung und Mustererkennung Gedanken lesen zu können. Kevin Brown, Softwarefachmann des amerikanischen Computerherstellers IBM, prognostiziert schon für das Jahr 2017 den flächendeckenden Einsatz von Hirn-Computer-Schnittstellen zum Beispiel beim Bedienen des Smartphones oder der Arbeit am Tablet PC. Das australische Hochtechnologie-Unternehmen Emotiv Systems verdient schon seit neun Jahren Geld mit seiner Hirn-Computer-Schnittstelle Epoc. Diese besteht aus 14 Elektroden, kostet 300 Dollar und wird zusammen mit einem dreidimensionalen Computerspiel der Demiurge Studios ausgeliefert. Softwarespezialisten wie Brown wollen daraus in den nächsten Jahre ein leistungsfähiges Peripherie-System machen, das es ihnen erlaubt, alle Arten von Computern allein mit Gedankenkraft zu bedienen.

Vorbild ist dabei die Spracherkennung. Schon heute kann die HiFi- und Klimaanlage im Auto durch mündliche Befehle gesteuert werden oder dem Smartphone zugerufen werden, wen wir anrufen wollen. Algorithmen für die Mustererkennung können unsere Sprache nahezu fehlerfrei in geschriebenen Text umsetzen oder Anweisungen erkennen und ausführen. Außerdem können sie schon heute bestimmte Muster unserer Hirnaktivität erkennen. Wenn wir intensiv daran denken, einen Würfel auf einem Bildschirm nach links zu bewegen, feuern unsere Synapsen entsprechende Impulse. Dies kann mit Elektroden gemessen werden. Das Geheimnis des Erfolges liegt im Training. So wie ein Spracherkennungssystem die einzelnen Sprachmuster eines Menschen lernen muss, benötigt die Software für Hirn-Schnittstellen Übung, um die Aktivitätsmuster zu erkennen, die entstehen, wenn Synapsen bei bestimmten Gedanken oder Gedankenfolgen aktiv sind.

Der Computeranwender geht dabei ähnlich wie beim Training von Diktier-Software vor, indem er beim Einarbeiten einer Hirn-Computer-Schnittstelle keinen Mustertext vorliest, sondern vorgegebene Gedankenfolgen abarbeitet. In den Forschungslaboratorien von Computerherstellern und Militärs werden derzeit rund 30 Aktivitätsmuster für die Bewegungssteuerung des Cursors und für die Bedienung von standardisierter Software trainiert. Brown hat im März 2009 angefangen, sich mit dieser Art der Mustererkennung von feuernden Synapsen zu beschäftigen. Damals erlitt ein Kollege im Forschungslabor einen Hirnschlag und wies infolgedessen ein sogenanntes Lock-In-Syndrom auf. Er hatte also keine Kontrolle mehr über seine Muskeln, konnte nicht mehr sprechen oder gestikulieren. Lediglich die Pupillen konnte er noch bewegen. Brown vereinbarte mit seinem Kollegen, dass hochgerollte Pupillen „ja“ bedeuten sollen und nach unten gerollte Pupillen „nein“. So konnten sie sich fragmentarisch verständigen. Brown kaufte ein Epoc-Headset von Emotive und programmierte für seinen Kollegen Mustererkennungssoftware, die in der Lage war, bestimmte Hirnaktivitätsmuster zu lernen, so dass Browns Kollege sich über die Hirn-Computer-Schnittstelle mit einem kleinen Grundwortschatz verständigen konnte. „Das klappte viel besser als die Kommunikation über die Pupillenstellung“, meint Brown. Daraus wurde ein Entwicklungsprojekt in den Forschungslaboratorien der IBM. Dort arbeiten die Forschenden an kleineren und genauer arbeitenden Elektroden, die sie beispielsweise in eine Baseballkappe integriert haben, und an einer Mustererkennungssoftware, die Hirnaktivitätsmuster mit einer ähnlichen Genauigkeit erkennt wie Spracherkennungssoftware heutzutage gesprochene Sprache. Forschende der University of California in Berkeley tüfteln an regelrechten Hirnscannern, mit denen sie sogar Träume analysieren wollen.

Bis es so weit ist, müssen bei der Entwicklung noch praktische Schwierigkeiten gelöst werden. So liefern zum Beispiel sogenannte trockene Sensoren, die ohne Elektrolytflüssigkeit auskommen, noch nicht hinreichend stabile Signale im Bereich von fünf Millionstel Volt. Doch die Arbeiten in diesem Bereich machen Brown zufolge gute Fortschritte. An der State University in New York werden sogar kontaktlose Elektroden entwickelt. Auch die mathematischen Gleichungssysteme, die zur Erstellung der Hirnaktivitätsmuster verwendet werden, liefern derzeit recht grob aufgelöste Muster, an deren Verfeinerung die Forscher arbeiten. Denn je hochauflösender die Muster erkannt werden, umso mehr Kombinationsmöglichkeiten verschiedener Gedankenfolgen können die Algorithmen auflösen beziehungsweise erkennen. Für Brown und seine KollegInnen ist klar, dass in wenigen Jahren die Menschen mit ihrem Smartphone nicht mehr über ein Mikrofon und Spracherkennung kommunizieren werden, sondern über die Elektroden der Hirn-Computer-Schnittstelle. Statt des gesprochenen Befehls „Ruf zu Hause an“ soll dann schon der Gedanke genügen (Welchering www.faz.net 16.01.2012).

Gesichts-OP-resistente Mustererkennung

Informatiker der University of Notre Dame im US-Bundesstaat Indiana haben eine Software entwickelt, mit der Menschen per Gesichtserkennung auch dann erkannt werden können sollen, wenn sie gezielt ihr äußeres Aussehen, z.B. per Schönheitsoperation, verändern. Hintergrund der Innovation ist, dass viele Computermodelle das Gesicht als Einheit erfassen. Dies ist bei gezielten Gesichtsveränderungen nicht ideal, weil dann auch kleinere Eingriffe bereits die Gesamtwirkung eines Gesichts stark verändern können. Mit ihrem neuen Programm konzentrieren sich die Forschenden daher auf charakteristische Merkmale wie Augen und Mund, von denen einige auch nach einer Gesichts-OP regelmäßig unverändert bleiben (Der Spiegel 5/2012, 99).

Computer analysieren Sprechergefühle

Computer können Spracheingaben in Schriftzeichen umsetzen. Als Nächstes soll ihnen beigebracht werden, anhand der Stimme die Gefühlslage der Sprechenden zu erkennen. Erste Systeme sind bereits in Callcentern im Einsatz. Die in Callcentern eingesetzten Systeme sollen KundInnen aufspüren, bei denen sich ein Verkaufsgespräch lohnt. Die Funktionsweise erklärt Bin Yang, Professor am Institut für Signalverarbeitung und Systemtheorie an der Universität Stuttgart: „Wenn jemand traurig ist, spricht er meistens langsam und nicht so laut. Wenn jemand wütend, glücklich oder überrascht ist, hingegen lauter und schneller.“ Aus solchen Merkmalen wird ein digitales Sprachprofil berechnet. „Wir setzen ein mathematisches Verfahren zur Mustererkennung ein, so wie es auch bei Spracherkennung, einem Fingerabdruck oder Iris-Scan gemacht wird.“ Dieses Muster wird dann mit einer Datenbank verglichen, in der menschliche Bewertungen als Referenz gespeichert sind. So bekommt das System beigebracht, welche Merkmale auf was für eine Emotion schließen lassen. „Der erste, aufwendige Schritt ist also der Aufbau dieser Datenbank. Menschen müssen möglichst viele Sprachmuster bewerten.“ Yang sieht noch keine Möglichkeit, aus einer Sprachanalyse Lügen zu detektieren: „Aus den Emotionen in der Stimme darauf zu schließen, ob jemand lügt, ist dann ein anderes Paar Schuhe.“

Julia Hirschberg, IT-Professorin an der Columbia University, will genau diesen Zusammenhang herstellen. Sie arbeitet an Algorithmen, die anhand einer Sprachaufzeichnung erkennen sollen, ob ein Mensch gerade lügt oder die Wahrheit sagt. Dutzende Merkmale wie Lautstärke, Geschwindigkeit, Wortpausen und nervöses Lachen geben dem gemäß Hinweise auf eine Täuschung. In einem ersten Testversuch, bei dem Testpersonen zu Interviews eingeladen wurden und bewusst täuschen sollten, habe der Computer in 70 Prozent der Fälle Lügen erkannt - Menschen entdeckten nur 57 Prozent der Täuschungen. Ein funktionierender Lügendetektor nur auf Sprachbasis wäre eine kleine Revolution. Seit den siebziger Jahren fahnden forensische PsychologInnen bisher ergebnislos nach verräterischen Signalen. Zwar geben sich manche Lügner unfreiwillig durch viele „Ähms“ zu erkennen, andere hingegen lassen sich buchstäblich nichts anmerken. Auch Lügendetektoren, die unter anderem Puls und Hautwiderstand messen, kommen laut Studien in fast der Hälfte der Fälle zu falschen Ergebnissen. Als Beweise, etwa vor Gericht, taugen solche Ergebnisse kaum. Hirschberg sieht sich und ihre KollegInnen trotzdem auf einem guten Weg, zumindest besser zu verstehen, wie sich Emotionen in unserer Sprache widerspiegeln. Die vage Aussicht auf eine Software, die Hinweise auf eine Täuschung geben kann, beflügelt offenbar auch Geldgeber. Nach Presseberichten haben Hirschberg und ihre KollegInnen von der US-Luftwaffe knapp 1,5 Millionen Dollar Forschungsgelder erhalten. Dafür sollen sie nicht nur in englischen Sprachaufnahmen Emotionen verstehen, sondern auch auf Arabisch und Chinesisch (www.spiegel.de 07.12.2011).

Rechtsprechung

EuGH

Europarecht schützt Zugangsdienste vor Überwachungspflicht

In einem Rechtsstreit zwischen der Scarlet Extended SA, einem Anbieter von Internetzugangsdiensten, und SABAM, einer belgischen Verwertungsgesellschaft, deren Aufgabe es ist, die Verwendung von Werken der Musik von Autoren, Komponisten und Herausgebern zu genehmigen, entschied der Europäische Gerichtshof (EuGH) am 24.11.2011, dass europäisches Datenschutzrecht einer von einem nationalen Gericht erlassenen Anordnung entgegensteht, die zur Filterung gegen unzulässiges Herunterladen von Dateien verpflichtet (Az. C-70/10).

SABAM stellte im Jahr 2004 fest, dass Scarlet nutzende User über das Internet – ohne Genehmigung und ohne Gebühren zu entrichten – Werke über „Peer-to-Peer"-Netze herunterluden. Auf Antrag von SABAM gab der Präsident des Tribunal de Première Instance de Bruxelles (Belgien) Scarlet als Anbieter von Internetzugangsdiensten unter Androhung eines Zwangsgelds auf, diese Urheberrechtsverletzungen abzustellen, indem sie es ihren KundInnen unmöglich mache, Dateien, die ein Werk der Musik aus dem Repertoire von SABAM enthielten, in irgendeiner Form mit Hilfe eines „Peer-to-Peer"-Programms zu senden oder zu empfangen. Scarlet legte beim Cour d'Appel de Bruxelles Berufung ein und machte geltend, dass die Anordnung nicht unionsrechtskonform sei, weil sie ihr de facto eine allgemeine Pflicht zur Überwachung der Kommunikationen in ihrem Netz auferlege, was mit der Richtlinie über den elektronischen Geschäftsverkehr und den Grundrechten unvereinbar sei. Der Cour d'Appel fragte nun den EuGH, ob die Mitgliedstaaten aufgrund des Unionsrechts dem nationalen Richter erlauben können, einem Anbieter von Internetzugangsdiensten aufzugeben, generell und präventiv allein auf seine eigenen Kosten und zeitlich unbegrenzt ein System der Filterung der elektronischen Kommunikationen einzurichten, um ein unzulässiges Herunterladen von Dateien zu identifizieren.

Der EuGH wies darauf hin, dass Inhaber von Rechten des geistigen Eigentums gerichtliche Anordnungen gegen Vermittler wie die Anbieter von Internetzugangsdiensten beantragen können, deren Dienste von einem Dritten zur Verletzung ihrer Rechte genutzt werden. Die Modalitäten der Anordnungen sind Gegenstand des nationalen Rechts. Diese nationalen Regelungen müssen jedoch die sich aus dem Unionsrecht ergebenden Beschränkungen wie u. a. die Richtlinie über den elektronischen Geschäftsverkehr beachten, wonach nationale Stellen keine Maßnahmen erlassen dürfen, die einen Anbieter von Internetzugangsdiensten verpflichten würden, die von ihm in seinem Netz übermittelten Informationen allgemein zu überwachen. Der EuGH meinte, dass die fragliche Anordnung Scarlet verpflichten würde, eine aktive Überwachung sämtlicher Daten aller ihrer KundInnen vorzunehmen, um jeder künftigen Verletzung von Rechten des geistigen Eigentums vorzubeugen. Daraus folgt, dass die Anordnung zu einer allgemeinen Überwachung verpflichten würde, die mit der Richtlinie über den elektronischen Geschäftsverkehr unvereinbar ist. Außerdem würde eine solche Anordnung nicht die anwendbaren Grundrechte beachten.

Zwar ist der Schutz des Rechts am geistigen Eigentum in der Charta der Grundrechte der Europäischen Union (EU) verankert. Gleichwohl ergibt sich aus der Charta selbst wie aus der EuGH-Rechtsprechung, dass dieses Recht nicht schranken- und bedingungslos besteht. Vorliegend sollte eine Filterung eingerichtet werden, wonach im Netz des fraglichen Anbieters die Nutzung des Internetzugangsdienstes zeitlich unbegrenzt überwacht werden müsste. Hierin sah der EuGH eine qualifizierte Beeinträchtigung der unternehmerischen Freiheit von Scarlet, da es verpflichtet würde, ein kompliziertes, kostspieliges, auf Dauer angelegtes und allein auf seine Kosten betriebenes Informatiksystem einzurichten. Das Filtersystem könnte auch die Grundrechte seiner KundInnen beeinträchtigen, nämlich die durch die Charta der Grundrechte der EU garantierten Rechte auf den Schutz personenbezogener Daten und auf freien Empfang oder freie Sendung von Informationen. Die Anordnung hätte eine systematische Prüfung aller Inhalte sowie die Sammlung und Identifizierung der IP-Adressen der NutzerInnen bedeutet, die die Sendung unzulässiger Inhalte in diesem Netz veranlasst haben, wobei es sich bei diesen Adressen um personenbezogene Daten handelt. Die Anordnung könne zudem die Informationsfreiheit beeinträchtigen, weil dieses System möglicherweise nicht hinreichend zwischen einem unzulässigen Inhalt und einem zulässigen Inhalt unterscheiden kann, so dass sein Einsatz zur Sperrung von Kommunikationen mit zulässigem Inhalt führen könnte.

Nach Ansicht des EuGH beachtete die Anordnung nicht das Erfordernis eines angemessenen Gleichgewichts zwischen einerseits dem Recht am geistigen Eigentum und andererseits der unternehmerischen Freiheit, dem Recht auf den Schutz personenbezogener Daten und dem Recht auf freien Empfang oder freie Sendung von Informationen. Der EuGH gab folglich die Antwort, dass das Unionsrecht einer Anordnung an einen Anbieter von Internetzugangsdiensten entgegensteht, ein System der Filterung aller seine Dienste durchlaufenden elektronischen Kommunikationen, das unterschiedslos auf alle seine KundInnen anwendbar ist, präventiv, auf ausschließlich seine eigenen Kosten und zeitlich unbegrenzt einzurichten (PM Nr. 126/11 des Gerichtshof der Europäischen Union vom 24.11.2011).

BVerfG

Verwendung von Telekommunikationsdaten teilweise verfassungswidrig

Leitsätze

1. In der Zuordnung von Telekommunikationsnummern zu ihren Anschlussinhabern liegt ein Eingriff in das Recht auf informationelle Selbstbestimmung. Demgegenüber liegt in der Zuordnung von dynamischen IP-Adressen ein Eingriff in Art. 10 Abs. 1 GG.

2. Der Gesetzgeber muss bei der Einrichtung eines Auskunftsverfahrens sowohl Rechtsgrundlagen für die Übermittlung, als auch für den Abruf von Daten schaffen.

3. Das automatisierte Auskunftsverfahren der §§ 112, 111 TKG ist mit der Verfassung vereinbar. § 112 TKG setzt dabei für den Abruf eigene Ermächtigungsgrundlagen voraus.

4. Das manuelle Auskunftsverfahren der §§ 113 Abs. 1 Satz 1, 111, 95 Abs. 1 TKG ist in verfassungskonformer Auslegung mit dem Grundgesetz vereinbar. Zum einen bedarf es für den Abruf der Daten qualifizierter Rechtsgrundlagen, die selbst eine Auskunftspflicht der Telekommunikationsunternehmen normenklar begründen. Zum anderen darf die Vorschrift nicht zur Zuordnung dynamischer IP-Adressen angewendet werden.

5. Die Sicherheitsbehörden dürfen Auskünfte über Zugangssicherungscodes (§ 113 Abs. 1 Satz 2 TKG) nur dann verlangen, wenn die gesetzlichen Voraussetzungen für ihre Nutzung gegeben sind.

Der Erste Senat des Bundesverfassungsgerichts (BVerfG) hat ohne mündliche Verhandlung mit Beschluss vom 24.01.2012 entschieden, dass die Regelungen zur Speicherung und Herausgabe von Nutzerdaten, Passwörtern und PIN-Codes an Ermittlungsbehörden und andere staatliche Stellen teilweise das Grundrecht auf informationelle Selbstbestimmung verletzen und verfassungswidrig sind (Az. 1 BvR 1299/05). Das BVerfG macht Schluss mit der nach Ansicht der Kammer „verbreiteten aber umstrittenen Praxis", § 113 auch für Auskünfte über den Inhaber einer IP-Adresse heranzuziehen: Die Regelung „berechtigt ... nicht zu einer Zuordnung von dynamischen IP-Adressen", weil dies einen Eingriff ins Fernmeldegeheimnis darstelle. Der Gesetzgeber hat hier bis Juni 2013 Zeit, eine verfassungskonforme Neuregelung zu schaffen. Das Gericht hat zudem eine in § 113 Satz 2 geregelte spezielle Auskunftspflicht der Provider gegenüber Strafverfolgern und Geheimdiensten kassiert, die Zugangssicherungscodes wie Passwörter oder PINs betraf. Das ist nach Ansicht der Richter nicht mit dem Recht auf informationelle Selbstbestimmung vereinbar, „weil sie nicht den Anforderungen des Verhältnismäßigkeitsgrundsatzes genügt". Der Zugriff auf diese Daten sei in dem derzeit geregelten Umfang „für die effektive Aufgabenwahrnehmung dieser Behörden nicht erforderlich". Die Vorschrift erlaube den Behörden Zugriff, ohne die Voraussetzungen dafür zu regeln. Auch hier hat das Verfassungsgericht eine Übergangsfrist bis Ende Juni 2013 angeordnet.

Karlsruhe hat keine Einwände gegen die im Telekommunikationsgesetz (TKG) festgeschriebene Pflicht für Telekommunikationsanbieter, die persönlichen Daten zu Telefonnummern, E-Mail-Adressen oder anderen Anschlusskennungen zu speichern. Auch das über die Bundesnetzagentur abgewikkelte automatische Auskunftsverfahren etwa für Strafverfolgungsbehörden ist in den Augen der Verfassungshüter nicht zu beanstanden, weil der damit einhergehende Eingriff in das Recht auf informationelle Selbstbestimmung „nur von begrenztem Gewicht" sei (§§ 111, 112 TKG). Die Beschwerde richtete sich auch gegen § 113, soweit er alle Anbieter von Kommunikationsdienstleistungen (also etwa auch Krankenhäuser oder Hotels) verpflichtet, einer anfragenden Behörde direkt Auskunft zu erteilen, wenn dies „für die Verfolgung von Straftaten und Ordnungswidrigkeiten, die Gefahrenabwehr oder nachrichtendienstliche Aufgaben erforderlich ist". Hiergegen erklärte das BVerfG grundsätzlich keine Einwände, macht aber eine klare Ansage für die Auslegung dieser Regelung. In der Praxis seien dabei bisher Rechtsgrundlagen, die die Behörden allgemein zur Erhebung von Daten ermächtigten, als ausreichend angesehen worden. Das soll künftig nicht mehr ausreichen: „Die Vorschrift ist jedoch verfassungskonform so auszulegen, dass es für den Datenabruf spezieller fachrechtlicher Ermächtigungsgrundlagen bedarf".

Das novellierte Telekommunikationsgesetz war im Juni 2004 in Kraft getreten. Ein Jahr später hatten vier E-Mail-Provider und zwei Privatpersonen Verfassungsbeschwerden gegen das Telekommunikationsgesetz (TKG) eingelegt. Einer der Beschwerdeführer war Patrick Breyer aus Meldorf, Kandidat auf Listenplatz 4 für die Piratenpartei bei den Landtagswahlen in Schleswig-Holstein im Mai 2012. Die Internet-Unternehmen wandten sich gegen die Auflage, Überwachungsschnittstellen ohne Entschädigung auf eigene Kosten vorhalten zu müssen. Dagegen hielten es die Privatpersonen für „grob unverhältnismäßig", persönliche Daten der gesamten Bevölkerung auf Vorrat zu speichern, nur weil ein Bruchteil dieser Daten einmal nützlich sein könnte. 2006 hatte das Bundesverfassungsgericht die Beschwerde in Teilen abgewiesen. Karlsruhe beschränkte sich auf die Überprüfung von Teilen des angegriffenen Gesetzes.

Patrick Breyer, der als Jurist am Meldorfer Amtsgericht tätig ist, meinte, die Bundesjustizministerin müsse nun klarstellen, dass „Internetnutzer nur noch mit richterlicher Genehmigung und zur Verfolgung schwerer Straftaten identifiziert werden dürfen". Er kritisierte, dass Karlsruhe nichts gegen den „Identifizierungszwang für Mobilfunkkarten" getan habe. Der Bundesdatenschutzbeauftragte Peter Schaar sah sich durch die Entscheidung in seiner Kritik an dem Gesetz bestätigt. Bundesjustizministerin Sabine Leutheusser-Schnarrenberg (FDP) erklärte, die Entscheidung stärke den Grundrechtsschutz bei Telekommunikationsdaten. Das BVerfG habe „einmal mehr ein rot-grünes Sicherheitsgesetz beanstandet und die handwerklichen Mängel gerügt". Bayerns Justizministerin Beate Merk (CSU) forder-

te, die Defizite des Gesetzes, die sich „leicht korrigieren“ ließen, rasch zu beheben.

Interessant ist die Kritik von Heribert Prantl von der Süddeutschen Zeitung (SZ): „Karlsruhe ist müde; das Bundesverfassungsgericht hat sich offenbar bei seiner 60-Jahr-Feier verausgabt. Jedenfalls kommt schon wieder eine seltsam gewundene, schlecht formulierte und entschlussschwache Entscheidung vom dortigen Senat. ... Zu loben gibt es nicht so arg viel. Die Richter haben nichts gegen die Massenabfragen (derzeit 26,6 Millionen!) von Kommunikationsdaten gesagt. Nur dort und da hängen sie vor deren Nutzung ein wackliges Stoppschild. Mit den großen Entscheidungen der vergangenen Jahre, in denen das Gericht ein Sicherheitsgesetz nach dem anderen zerlegte, hat das wenig zu tun“ (www.heise.de 24.02.2012; KN 25.02.2012, 4; Kerscher u. Prantl SZ 25./26.02.2012, 1, 4).

BVerfG

Telekommunikationsüberwachungsnovelle verfassungsgemäß

Das Bundesverfassungsgericht (BVerfG) hat mit Beschluss vom 12.10.2011 mehrere Verfassungsbeschwerden gegen die 2008 in Kraft getretene Novelle der Telekommunikationsüberwachung aus dem Jahr 2007 zurückgewiesen (AZ: 2 BvR 236/08, 2 BvR 237/08, 2 BvR 422/08). Geklagt hatten unter anderem mehrere, vom Altliberalen Burkhard Hirsch vertretene FDP-Abgeordnete und VertreterInnen der Bürgerrechtsorganisation Humanistische Union. Die KlägerInnen kritisierten die unzureichende Sicherung des „absolut geschützten Kernbereichs privater Lebensgestaltung“, einen 2-Klassen-Schutz sogenannter Berufsgeheimnisträger und eine unangemessene Ausweitung des Straftatenkatalogs. Der Zweite Senat des Bundesverfassungsgericht unter dem Präsidenten Andreas Voßkuhle ließ keinen der vorgebrachten Gründe gelten.

Das BVerfG bestätigt das neue zweistufige Konzept, das Abgehörte vor Eingriffen in ihre Intimsphäre bewahren soll. Entgegen der Auffassung der BeschwerdeführerInnen müssten Überwachungsmaßnahmen nicht schon deshalb unterlassen werden, „weil auch Tatsachen mit erfasst werden, die auch den Kernbereich des Persönlichkeitsrechts berühren“. Ein umfassendes Erhebungsverbot würde die TK-Überwachung in einem Maße einschränken, „dass eine wirksame Strafverfolgung gerade im Bereich schwerer und schwerster Kriminalität nicht mehr gewährleistet wäre“. In vielen Fällen sei es „praktisch unvermeidbar“, dass die Behörden die Schutzwürdigkeit äußerst persönlicher Gespräche erst im Nachhinein entdeckten - zumal bei Gesprächen, die in fremden Sprachen geführt werden. Der Schutz des Kernbereichs sei durch einen „hinreichenden Grundrechtsschutz in der Auswertungsphase“ sicherzustellen. Sollten bei einer Abhörmaßnahme Daten erfasst werden, die die absolut geschützte Intimsphäre berührten, greife das Verwertungsverbot. Im Lauschangriff-Urteil von 2004 hatte das BVerfG noch kategorisch das sofortige Abschalten der Überwachung angeordnet, sobald der „Kernbereich“ berührt wird.

Der Gesetzgeber habe zudem den Katalog der Straftaten in § 100a StPO, bei denen abgehört werden darf, „nicht in verfassungswidriger Weise in die Bereiche der leichten und mittleren Kriminalität hinein ausgedehnt“. Aus dem früheren Katalog waren 19 Straftatbestände gestrichen, in den neuen mehr als 30 aufgenommen worden - und zwar solche mit einer Höchststrafe von 5 Jahren und mehr. Die Gesetzesreform ermöglicht die Überwachung etwa auch bei Korruptionsdelikten, schweren Steuervergehen oder Verbreitung, Erwerb und Besitz von Kinderpornografie. Dies qualifiziere die Delikte noch nicht als schwere Straftaten, bei denen ein Eingriff in Art. 10 GG verhältnismäßig sei. „Eine Höchststrafe von fünf Jahren ist im Strafgesetzbuch der Regelfall.“ Bei einer „Gesamtschau“ sei die Einschätzung des Gesetzgebers als „schwerwiegend“ allerdings vertretbar, zumal ein pauschaler Verweis auf die Liste nicht für die Telefonüberwachung genüge, sondern die Taten „auch im Einzelfall“ schwerwiegend sein müssten.

Für grundgesetzkonform hält Karlsruhe auch das überarbeitete Modell zum Schutz von Zeugnisverweigerungsberechtigten in § 160a StPO. Ein absolutes Beweiserhebungs- und Verwendungsverbot gilt demnach für Abgeordnete, Seelsorger und Strafverteidiger sowie seit Februar 2011 auch für die übrigen Rechtsanwälte. Andere Berufsgeheimnisträger wie ÄrztInnen oder JournalistInnen dürfen dagegen „nach Abwägung der Verhältnismäßigkeit“ überwacht werden. Mit der Begrenzung des absoluten Schutzes auf wenige Ausnahmefälle trage der Gesetzgeber dem Umstand Rechnung, „dass die Verfolgung von Straftaten hohe Bedeutung hat“.

Das BVerfG bestätigte weiterhin die überarbeitete Regelung in § 101 Abs. 4 bis 6 StPO, ob und wann Betroffene über erfolgte verdeckte Ermittlungsmaßnahmen zu informieren sind. Der Anspruch darauf gehöre zwar zum effektiven Grundrechteschutz. Ausnahmen könnten aber in Abwägung mit verfassungsrechtlich geschützten Rechtsgütern Dritter vorgesehen werden. Unterbleiben könne eine Benachrichtigung etwa, „wenn die Kenntnis des Eingriffs in das Telekommunikationsgeheimnis dazu führen würde, dass dieser seinen Zweck verfehlt“ (PE BVerfG 07.12.2011; Krempl www.heise.de 07.12.2011; Janisch SZ 08.12.2011, 5).

BVerfG

Kein Verwertungsverbot bei illegalem Lauschangriff

Das Bundesverfassungsgericht hat mit Beschluss vom 07.12.2011 die Verurteilung von drei Al-Qaida-Aktivisten wegen Versicherungsbetrug aufgehoben, weil die Schadenhöhe nicht korrekt ermittelt worden ist. Die Verwertung von Erkenntnissen aus einem Lauschangriff wurde dagegen nicht beanstandet (Az. 2 BvR 2500/09, 2 BvR

1857/10). Mit dem Versicherungsbetrug wollten die Islamisten Mittel für das Terrornetzwerk Al-Qaida beschaffen. Hierzu schloss der Palästinenser Yasser Abu-S. im Sommer 2004 zahlreiche Lebensversicherungen ab. Bei einer späteren Urlaubsreise sollte mit Unterstützung von korrupten ägyptischen Beamten sein Tod vorgetäuscht werden; die Versicherungssumme von 4 Mio. Euro sollte der Terrorfinanzierung dienen. Angestiftet wurde er durch den Syrer Ibrahim Mohamed K. Geholfen hatte außerdem ein Bruder von Yasser Abu-S. Die drei wurden 2007 vom Oberlandesgericht Düsseldorf zu mehrjährigen Haftstrafen verurteilt. Der Bundesgerichtshof (BGH) bestätigte das Urteil im Wesentlichen. Die Verurteilung der drei beruhte auf Erkenntnissen einer fünfmonatigen akustischen Überwachung der Wohnung von Ibrahim Mohamed K. in Mainz. Aus 304 Stunden Lauschangriff wurden 313 Gespräche übersetzt. Die Maßnahme diente zunächst der Gefahrenabwehr und wurde auf das rheinland-pfälzische Polizeigesetz gestützt. Doch dieses Gesetz enthielt damals noch keine Vorschriften zum Schutz des Kernbereichs privater Lebensgestaltung und war deshalb teilweise verfassungswirdig.

Dennoch hielt der BGH und nun das BVerfG die Ergebnisse des Lauschangriffs für verwertbar. Das Recht auf ein faires Strafverfahren sei nicht verletzt. Auch rechtswidrig erlangte Informationen könnten vor Gericht als Beweismittel genutzt werden. Das BVerfG bemängelte jedoch, dass der BGH zur Höhe des Schadens nur vage Äußerungen machte. Konkrete Angaben seien schon deshalb erforderlich, weil die Versicherungssumme noch nicht bezahlt worden war und nur eine Gefährdung des Vermögens der Versicherungen erfolgte. Der BGH muss nun erneut über den Fall entscheiden. Selbst wenn eine Verurteilung wegen Versicherungsbetrug nicht möglich sein sollte, bliebe eine Bestrafung wegen Mitgliedschaft und Unterstützung einer terroristischen Vereinigung bestehen (Rath taz 30.12.2011, 6; BVerfG PM 29.12.2011)

BGH

Mutter muss Scheinvater wahren Erzeuger von Kuckuckskind nennen

Der Familiensenat des Bundesgerichtshofes (BGH) hat mit Urteil vom 09.11.2011 entschieden, dass Männer, denen ein sog. Kuckuckskind untergeschoben worden ist, von der Mutter Auskunft über den Namen des wahren Erzeugers verlangen können (Az. XII ZR 136/09). Ein pensionierter 49jähriger Polizeibeamter hatte für seinen vermeintlichen Sohn knapp 4.575 Euro Unterhalt gezahlt und wollte das Geld nun von dem - ihm unbekannten - leiblichen Vater zurückfordern. Diese Klage des „Scheinvaters" war in allen drei Instanzen erfolgreich, zuletzt beim Oberlandesgericht Schleswig-Holstein. Er hatte die Vaterschaft zunächst im Januar 2007 vor der Geburt des Kindes anerkannt, obwohl die Beziehung schon nach ständigen Streitereien beendet war. Als während eines Prozesses ein Vaterschaftsgutachten eingeholt wurde, stellte das Familiengericht fest, dass der Kläger nicht der Vater sei. Dies gab er in der Regionalzeitung öffentlich bekannt.

Der BGH gründete den Auskunftsanspruch auf „Treu und Glauben" - weil der Scheinvater die Vaterschaft letztlich auf Betreiben der Mutter anerkannt hatte. Die Senatsvorsitzende Meo-Micaela Hahne hatte in der Verhandlung angedeutet, dies sei relevant, „auch wenn man der Mutter zugestehen mag, dass sie den Kläger für den Vater hielt". Die Frau hatte die Preisgabe des Namens des biologischen Vaters unter Berufung auf den Schutz ihrer Privat- und Intimsphäre verweigert. Der Anwalt der Mutter, Siegfried Mennemeyer, meinte der falsche Vater hätte seine Vaterschaft von vornherein klären müssen: „Er hätte einfach nicht zahlen müssen". Der BGH ließ dies nicht gelten. Die Mutter habe ja bereits zuvor einen Mann, mit dem sie intim gewesen sei, als Vater offenbart - nur eben den falschen. In diesem Fall wiege ihr Persönlichkeitsrecht nicht stärker als der Anspruch des Mannes auf eine wirksame Durchsetzung seines Regressanspruchs.

Auf Grund eines Urteils des Bundesverfassungsgerichts aus dem Jahr 2007 kann ein zweifelnder Vater die Klärung der biologischen Vaterschaft auch gegen den Willen der Mutter herbeiführen (DANA 1/2007, 37 f.). Bis zur aktuellen BGH-Entscheidung war aber die Frage des Auskunftsanspruchs des Scheinvaters ungeklärt. Vor 1998 waren auch die Jugendämter mit solchen Fällen befasst und konnten im Konfliktfall für Klarheit sorgen. Seit der sog. Kindschaftsrechtsreform sind die Ämter aber außen vor. Die BGH-Entscheidung war absehbar: Anfang 2011 hatte etwa das Amtsgericht Bonn entschieden, dass ein Telekommunikationsunternehmen Name und Anschrift eines Kunden herausgeben muss, wenn ein Kind wissen will, wer sein leiblicher Vater ist, die Mutter aber von ihrem damaligen Sexualpartner nur den Vornamen und die Handynummer kennt (SZ 10.11.2011, 5; Janisch SZ 09.11.2011, 1; Hipp, Der Spiegel 45/2011, 44 f.; vgl. DANA 3/2011, 131).

BGH

Polizeilich abgehörte Selbstgespräche sind absolut nicht verwertbar

Der Bundesgerichtshof (BGH) hat mit Urteil vom 22.12.2011 entschieden, dass ein im Selbstgespräch gemachtes Geständnis eines Mörders, der sich allein und unbelauscht wähnt, zum absolut geschützten Kernbereich der Privatsphäre gehört und damit vor Gericht unverwertbar ist, wie schwer auch immer der Vorwurf sei (2 StR 509/10).

Der Mitbeschuldigte Siegfried K. und seine philippinische Ehefrau Lotis R. hatten einen Sohn; eines Tages trennten sie sich, was aber K´s Zwillingsschwester und ihrem Mann missfiel. Sie hatten den Jungen liebgewonnen und wollten ihn behalten, kämpften vor Gericht um ein eigenes Umgangsrecht und boten der Mutter sogar Geld. Im April 2007 verschwand die Mutter und wurde bis heute nicht gefunden. Nach Ansicht des Landgerichts (LG) Köln war die Mutter von dem Trio ermordet worden. Beweismittel war ein per Wanze aufge-

zeichnetes Selbstgespräch von Siegfried K. im Auto: „Die Lotis ist schon lange tot. Oho I kill her. ... Wir haben sie totgemacht.“ Nach der Entscheidung des BGH hätte das LG Köln den Monolog nicht verwerten dürfen, so Strafsenatsvorsitzender Thomas Fischer: „Der Grundsatz, dass die Gedanken frei und dem staatlichen Zugriff nicht zugänglich sind, beschränkt sich nicht auf innere Denkvorgänge“. Der Schutz gründe in der Menschenwürde und umfasse das Aussprechen von Gedanken im Selbstgespräch, bei dem sich jemand „als allein mit sich selbst empfindet“. Das absolute Verwertungsverbot wirkt auch in Bezug auf die beiden Mitangeklagten. 1989 hatte das Bundesverfassungsgericht (BVerfG) den staatlichen Einblick in innere Vorgänge noch erlaubt: In einer Vier-zu-Vier-Entscheidung hatten sie Tagebuchaufzeichnungen als verwertbar erklärt. Nach Ansicht des BGH ist aber ein bruchstückhafter „Gedankenfluss“ ungleich persönlicher als schriftlich fixierte Gedanken.

Maßgeblich waren die Umstände des konkreten Falles. Nicht jedes Selbstgespräch einer Person sei ohne Weiteres dem vor staatlichen Eingriffen absolut geschützten Kernbereich der Persönlichkeit zuzuordnen. Nach den Grundsätzen des Schutzes der Menschenwürde und der Freiheit der Person müsse ein Kernbereich privater Lebensgestaltung und Lebensäußerung verbleiben, in welchen der Staat auch zur Aufklärung schwerer Straftaten nicht eingreifen darf. Wichtige Kriterien für die Entscheidung, ob Äußerungen in Selbstgesprächen dem innersten, unantastbaren Bereich der Persönlichkeit zuzuordnen sind, seien

- die Eindimensionalität der Selbstkommunikation, also die Äußerung ohne kommunikativen Bezug;
- die Nichtöffentlichkeit der Äußerungssituation und das Maß des berechtigten Vertrauens der Person darauf, an dem jeweiligen Ort vor staatlicher Überwachung geschützt zu sein;
- die mögliche Unbewusstheit der verbalen Äußerung;
- die Identität der Äußerung mit den inneren Gedanken,
- die Äußerungsform als bruchstückhafter, auslegungsfähiger oder -bedürftiger Ausschnitt eines „Gedankenflusses“.

In der Flüchtigkeit und Bruchstückhaftigkeit des in Selbstgesprächen gesprochenen Worts ohne kommunikativen Bezug liegen nach Ansicht des Senats auch rechtlich erhebliche Unterschiede etwa zu Eintragungen in Tagebüchern. Aus dem Umstand, dass eine Äußerung innerhalb des nach Art. 13 GG geschützten Bereichs der Wohnung fällt, lässt sich nach der gesetzlichen Systematik zwar ein verstärkendes Indiz für die Zuordnung zum geschützten Kernbereich ableiten. Auch außerhalb der Wohnung ist dieser Kernbereich aber absolut geschützt, wenn andere der genannten Gesichtspunkte in der Wertung überwiegen. So lag es in dem vom 2. Strafsenat entschiedenen Fall. Der gegen die Zuordnung zum Kernbereich der Persönlichkeit sprechende Sozialbezug der Äußerungen, der in ihrem möglichen oder tatsächlichen Bezug auf eine schwere Straftat lag, trat dagegen zurück.

Es ist unklar, ob der Mord damit ungesühnt bleibt. Es gebe, so Fischer, „erhebliche Indizien“, die möglicherweise für eine Verurteilung reichten. Das muss das LG Köln klären, an das der Fall zurückverwiesen wurde (BGH PM Nr. 206/2011 v. 22.12.2011; Janisch SZ 23.12.2011, 1).

OLG München

Keine Herausgabepflicht von Nutzungsdaten bei illegalem Upload

Das Oberlandesgericht (OLG) München hat mit Beschluss vom 17.11.2011 in zweiter Instanz entschieden, dass YouTube keine Daten von Nutzenden herausgeben muss, die illegal Filmmaterial auf die Plattform laden, dabei aber keine kommerziellen Ziele verfolgen (Az. 29 U 3496/11). Ein Filmverleih beantragte eine einstweilige Verfügung, weil YouTube keine Auskünfte über einen User geben wollte, der große Teile des Kinofilms „Werner Eiskalt“ ins Internet gestellt hatte. Zwar habe der Nutzer eindeutig gegen das Urheberrecht verstoßen. Auskünfte über denjenigen, der das Video veröffentlichte, könnten dem Gesetz nach aber nur dann vom Rechteinhaber eingefordert werden, wenn der Nutzer das „in gewerblichem Ausmaß“ getan habe. Dies sei im vorliegenden Fall nicht zu erkennen. Zuvor hatte bereits das Landgericht München ebenso entschieden.

Der Nutzer hatte die Videos vermutlich im Kinosaal aufgenommen und sechs Sequenzen aus dem erfolgreichen Comic-Film beim Portal hochgeladen. Das sei „über die Hälfte des Films“ gewesen, so der Constantin-Anwalt Björn Frommer. YouTube hatte die Videos im Sommer auf Verlangen des Filmverleihs unverzüglich aus dem Netz entfernt. Gegen die Entscheidung des Oberlandesgericht im Eilverfahren gibt es kein weiteres Rechtsmittel. Die beiden Parteien erwägen nun, die Frage im Hauptsacheverfahren umfassend prüfen zu lassen (www.zeit.de 18.11.2011; medienrecht-blog.com 24.11.2011).

VG Düsseldorf

Verfassungsschutz muss Datenverarbeitung neu ordnen

Die geheimdienstlich Beobachtung und Ausforschung des Rechtsanwalts und Publizisten Rolf Gössner durch den Verfassungsschutz (VS) von Nordrhein-Westfalen (NRW) war gemäß dem rechtskräftigen Urteil des Verwaltungsgerichts (VG) Düsseldorf vom 19.10. 2011 unzulässig (Az. 22 K 4905/08). Der Prozess hatte 3½ Jahre gedauert. Anfang 2011 hatte das VG Köln die vier Jahrzehnte lange Überwachung Gössners durch das Bundesamt für Verfassungsschutz (BfV) für unverhältnismäßig und grundrechtswidrig erklärt (DANA 1/2011, 36f.). Das Gericht wirft dem VS NRW vor, eingrenzende gesetzliche Bestimmungen nicht eingehalten und vor allem die Datennutzung nicht effektiv kontrolliert und protokolliert zu haben. Nach Auffassung des Prozessbevollmächtigten von Rolf Gössner, des freiburger Anwalts Udo Kauß (Humanistische Union), wird dieses Urteil bundesweit erhebliche Auswirkungen auf die Datenverarbeitung aller 17 VS-Ämter des Bundes und der Länder haben. Udo Kauß: „Erstmals

wird eine Geheimdienstbehörde durch ein Gericht verpflichtet, ihre Datenverarbeitung so zu organisieren, dass die VS-Bediensteten nur auf die gespeicherten Daten zugreifen können, auf die das Gesetz für die jeweilige Aufgabe einen Zugriff erlaubt.“ Das Gericht hat den VS auch verpflichtet, durch technische Vorrichtungen sicher zu stellen, dass die Rechtmäßigkeit eines jeden Datenzugriffs im Nachhinein jederzeit überprüft werden kann. Sind diese Voraussetzungen nicht erfüllt, so Kauß, „dann ist jegliche Speicherung und jeglicher Zugriff rechtswidrig und ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung des Betroffenen“.

Der VS NRW hatte über Rolf Gössner eine Personendatei mit Personalien und Kontakten zu bestimmten Gruppen und Personen angelegt, die im Verfahren aus Geheimhaltungsgründen/ Quellengefährdung nur geschwärzt vorgelegt wurden. In 9 elektronischen Dokumenten (Sachdatei) waren Veranstaltungen des Klägers in NRW sowie Daten zu „linksextremistischen Bestrebungen bzw. Verdachtsfällen“ registriert, des Weiteren Gespräche, Äußerungen Dritter über Gössner, Protokolle und Berichte über Treffen bzw. Sitzungen „linksextremistischer“ Bestrebungen und Informationen über Aktionen und künftige Vorhaben. Die Daten beruhten u. a. auf „Quellenberichten“ von V-Leuten und anderen geheimen Informanten des VS, so etwa Erkenntnisse über einen nicht namentlich genannten Verein, in dem Rolf Gössner Vorstandsfunktionen innehatte und der angeblich von Personen „unterwandert“ werden sollte; diese sollen einer Organisation angehört haben, die in der EU-Terrorliste geführt wird. Deshalb war Gössner über ein ganzes Jahr selbst Gegenstand direkter verfassungsschützerischer Überwachung. Der Verdacht habe sich jedoch nicht erhärtet. Erfasst wurde zudem die Tatsache, dass Rolf Gössner u. a. für die Internationale Liga für Menschenrechte an der Beobachtung eines Prozesses vor dem Verwaltungsgerichtshof (VGH) Mannheim teilgenommen hatte, in dem es um ein Berufsverbot für einen Realschullehrer in Baden-Württemberg ging. Der VGH erklärte dieses vom baden-württembergischen Verfassungsschutz begründete und vom Kultusministerium verhängte Berufsverbot für rechtswidrig und hob es auf. Der Prozessbeobachter Gössner blieb in NRW weiterhin erfasst.

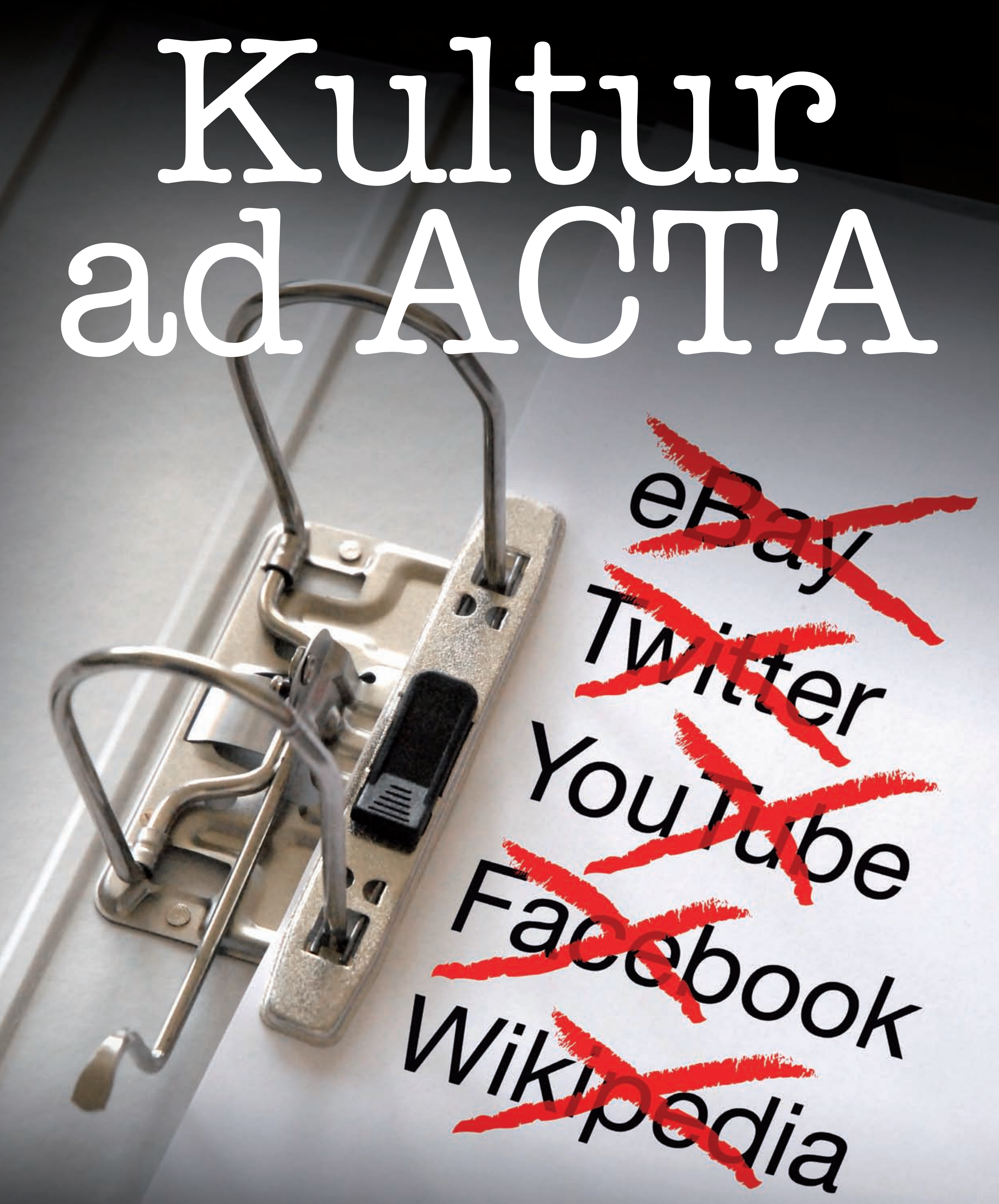
Zu den erfassten Veranstaltungen in NRW, auf denen Rolf Gössner als Referent aufgetreten war, gehörten die des Duisburger „Netzwerkes gegen Rechts“ und Vorträge des Klägers zu Themen wie „Innere Sicherheit“, „V-Leute in Neonaziszenen“ oder „Abbau von Menschenrechten“; die VS-Berichte enthielten Angaben zur Vergütung, die der Kläger für einen Vortrag erhalten habe, sowie die Wiedergabe längerer, nicht-öffentlicher Ausführungen eines dem „linksextremistischen Spektrum“ zuzurechnenden Redners zum gescheiterten NPD-Verbotsverfahren; darin komme der Satz vor: „Etwa 30 der 200 NPD-Vorstandsmitglieder waren Geheimdienstler, das Peinliche war nur, dass sie – nach Rolf Gössner – an Brandstiftung, Totschlag, Mordaufrufen, Waffenhandel, Gründung einer terroristischen Vereinigung direkt beteiligt waren“.

Das Verwaltungsgericht Düsseldorf hat mit seinem Urteil die gesamte Datenerfassung, -speicherung und -verarbeitung des Verfassungsschutzes NRW im Fall Gössner für rechtswidrig erklärt, weil nicht kenntlich gemacht wurde, ob dieser selbst verdächtiges Objekt war - in den Worten des VS: „doloses Objekt“, also mutmaßlicher „Verfassungsfeind“ oder „Extremist“ - oder aber eine „undolose“ Kontaktperson, die selbst keine „verfassungsfeindlichen Bestrebungen“ verfolgt. Obwohl Gössner gerade nicht als Teil einer „linksextremistischen Bestrebung“ erfasst worden war, habe er mangels korrekter Kennzeichnung als „belastete Person“ gegolten und seine Daten hätten etwa gesetzeswidrig bei Sicherheitsüberprüfungen Verwendung finden können. Auch die Tatsache, dass Daten über Gössner in sog. Sachdatenbanken nach Belieben namentlich recherchierbar waren, verstieß gegen geltendes Recht. Mit diesen Praktiken sei einer verbotenen zweckwidrigen Weiterverwendung von personenbezogenen Daten unkontrollierbar Tür und Tor geöffnet worden (PM Internationale Liga für Menschenrechte, Humanistische Union, 13.12.2011).

LG Lüneburg

Postwurfsendung bei Widerspruch unzulässig

Gemäß Urteil des Landgerichts (LG) Lüneburg vom 30.09.2011 stellt die Zusendung nicht gewünschter Postwurfsendungen einen Eingriff in das Recht auf informationelle Selbstbestimmung dar. Ein Verbraucher ist nicht gezwungen, einen Aufkleber mit den Worten „Werbung - Nein Danke“ auf seinem Briefkasten anzubringen. Vielmehr genügt es, wenn er dem Unternehmen mitteilt, dass er eine derartige Werbung nicht wünscht (Az.: 4 S 44/11). Der Kläger erhielt regelmäßig in seinen Briefkasten die Zeitschrift der Deutschen Post „Einkauf aktuell“ eingeworfen. Diese Postwurfsendung besteht aus einem wöchentlichen TV-Programmhaft und Werbebroschüren unterschiedlicher Handelsunternehmen. Als er die Post aufforderte, dies zu unterlassen, lehnte diese ab und wies darauf hin, dass er einen entsprechenden „Werbung, nein danke“-Aufkleber an seinen Briefkasten anbringen könne. Das LG Lüneburg teilte diese Ansicht nicht und verurteilte das Unternehmen zur Unterlassung. Es handele sich um unerlaubte Werbung, die das Allgemeine Persönlichkeitsrecht des Klägers verletze. Der Kläger habe sich mehrfach an die Beklagte gewandt und darum gebeten, die Postwurfsendungen sein zu lassen. Trotz dieser Kenntnis habe die Beklagte die Werbung weiterhin in den Briefkasten geworfen. Der Kläger müsse sich nicht darauf verweisen lassen, dass er einen Aufkleber mit den Worten „Werbung - Nein Danke“ anbringen solle. Es reiche aus, dass er dem Unternehmen mitteile, keine Postwurfsendungen mehr erhalten zu wollen (KN 07.01.2012, 7; dejure.org; dr-bahr.com 21.12.2011).



EU-Kommissar Karel De Gucht:

„Unsere Verantwortung als Politiker ist, Tatsachen zu schaffen und nicht der Masse folgen"

http://www.europarl.europa.eu/news/de/pressroom/content/20120227IPR39340/html/ACTA-MEPs-want-clarity-before-taking-a-decision

Grafik: Frans Valenta